Computer PANORÁMA

Computer Panoráma
XIV. évfolyam 14. különszám, 2003. október
Ára: 695 Ft

HACKER

Hackerek, crackerek, védelem

KÜLÖNSZÁM

CD-melléklettel

Minden feltörhető!
A hacker világ titkai

Letöltés ingyen
Filmek, zenék, programok

Ne mondd meg, kitalálom
Jelszavak feltörése

Hamisítás felső fokon
Bankkártyák, hitelkártyák

Megállj a betolakodóknak
A legjobb tűzfalak

Kevin Mitnick
Hogyan él egy hacker?

Cracker módszerek
Keygen, patch, serial, warez

Falbontási technikák
Tűzfalak kicselezése

Filmvilág
Hollywood és a hackerek

A CD tartalmából:
Titkosító programok
Jelszónyilvántartók
Antivírus programok
Tűzfalak

Járja be velünk a hackerek titkos világát!

03014
9 770865 524126

Hogy ne kelljen sokat költenie, mégis legyen házimozija!

PC & MOZI

- Tévé és videó a PC-n
- Képmagnó a PC-ből
- Sztereó helyett: térhangzás
- A PC mint DVD-lejátszó
- A leghasznosabb tippek és trükkök

CD-melléklettel

Ára: 3990 Ft

Rendelje meg most!

Telefon: 456-6963, Fax: 456-6970
Internet: www.computerpanorama.hu/pcmozi
E-mail: megrendeles@cpanorama.hu

Megrendelését 2 héten belül teljesítjük!
A megrendelt könyveket utánvéttel küldjük, áraink a postaköltséget nem tartalmazzák!
(A postaköltséget az érvényes postai díjszabás szerint számoljuk.)

IMPRESSZUM

HACKER
A Computer Panoráma különszáma
XIV. évfolyam 14. különszám, 2003. október

Felelős szerkesztő: Kazári Csaba
Szerkesztő: Horváth Annamária
Tördelőszerkesztő: Dancs Katalin
Címlap: Szincsák László

■ **Szerkesztőség:**
1091 Budapest, Üllői út 25. I. em.
Telefon: 456-6888, fax: 456-6970
E-mail: c.panorama@cpanorama.hu
Internet: http://www.computerpanorama.hu

■ **Kiadó: Computer Panoráma Kiadói Kft.**
Felelős kiadó: Dely Tamás ügyvezető igazgató
1091 Budapest, Üllői út 25. I. em.
Telefon: 456-6888

■ **Terjesztés:**
Mosolygó Kitti marketing- és terjesztési vezető
1091 Budapest, Üllői út 25. I. em.
Telefon: 456-6964, fax: 456-6970, e-mail: terjesztes@cpanorama.hu

■ **Ügyfélszolgálat, hétfő–péntek: 9–17 óráig**
Terjeszti: a Lapker Rt., az alternatív terjesztők és a Kiadó – Előfizetésben terjeszti a Magyar Posta Rt.

Hirdetésfelvétel:
hirdetési vezető: Tasnádi Rózsa
hirdetésszervező: Kuba Ilona, Háder Judit
1091 Budapest, Üllői út 25. I. em.,
Telefon/fax: 456-6974, fax: 456-6970
E-mail: hirdetes@cpanorama.hu

■ **Előfizetés:** a kiadónál személyesen, levélben, e-mailben, weboldalunkon vagy a postahivatalokban, a hírlapkézbesítőknél és a Hírlap-Előfizetési és Elektronikus Posta Igazgatóságon (HELP) 1900 Bp. XIII., Lehel út 10/A, a Postabank Rt. 219-98636/021-12799 pénzforgalmi jelzőszámon. Előfizethető OTP bankkártyával a 266-0000 telefonszámon (H–Szo, 9–20 óráig).

■ **A HACKER különszámot készítette:**
Levilágítás: HVG Press
Nyomtatás: Pauker Nyomdaipari Kft.
1047 Budapest, Baross u. 11–15.
Felelős vezető: Vértes Gábor ügyvezető igazgató

ISSN 0865-5243

Tisztelt Olvasó!

Divatos téma rengeteg létezik – valóságshow-k, sztárok magánélete, bankbotrányok, s nincs ez másképp a számítástechnikában sem, ahol a legtöbbet az MP3-ról, a DVD-ről és a DivX-ről, illetve a hackerekről beszélnek. A legtöbb esetben azonban a „divatos" vagy népszerű téma nem jelenti azt, hogy a vonatkozó írások szolgálnak is valamiféle hasznos információval. Ez a jelenség legélesebben a hacker/cracker témakörben körvonalazódik: rengeteget olvashatunk hackerekről, szerverek feltöréséről, honlapok átalakításáról, izgalmas és érdekes hacker-találkozókról, jelszavak ellopásáról és egyebekről – ritkábban kapunk azonban mélyreható elemzést arról, hogy valójában hogyan is ügyködnek a számítógép feltörői. Egyáltalán, miért teszik mindezt? És persze ami a legfontosabb: miként védekezhetünk a rosszindulatú „behatolók" és a kíváncsiskodók ellen? Hogyan védhetjük meg hatásosan az adatainkat és a munkánkat?

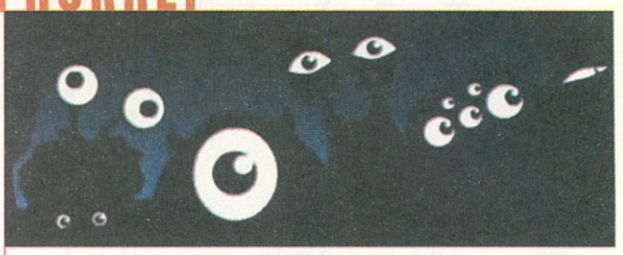
Bizonyára mindenki emlékszik több-kevesebb esetre, amikor a hackerek/crackerek és a számítógépes biztonság hirtelen a figyelem középpontjába kerültek: gondoljunk csak az Elender híres-hírhedt „feltörésére", a pécsi „warez" letartóztatásokra, a BRFK honlapjának megmásítására vagy akár egy nemrégiben zajló levélváltásra egy hacker és a Symantec Rt. között. Mindenezen esetek idővel elfelejtődnek, a céges és magánszféra hálózati biztonsága pedig marad olyan-amilyen: többnyire kritikán aluli. Ez persze nem helyes, hiszen nekünk, magyaroknak is vannak „hackereink", jók és rosszak egyaránt – csak valahogy nem veszünk tudomást róluk, pedig kellene...

Persze a hatásos védekezés (akárcsak az orvostudományban) azon a tényen alapszik, hogy megismerjük és megértsük azt, amitől tartunk, ami ellen védekezni kívánunk. Felesleges tehát tanácsokat és „aranyszabályokat" hangoztatni addig, amíg nem vagyunk teljesen tisztában azzal, mi is az, amitől félnünk kell, és mi az, amitől nem.

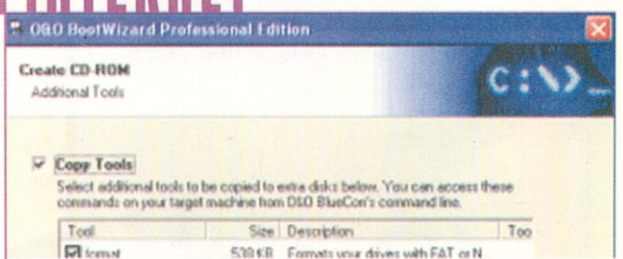
Jelen különszámunknak pedig éppen ez a célja: ne csak hangzatos, érdekes sztorikat és anekdotákat, esetleg ködös elemzéseket közöljünk a hackerekről, ismerjük meg konkrétan: hogyan és miként is dolgoznak. Ezután pedig (ezzel az újonnan megszerzett tudással felvértezve) beszéljünk a lehetséges védekezési módokról, eljárásokról és trükkökről. Magyarországon szerencsére a „jó" hackerek vannak túlnyomó többségben, megijednünk tehát nem, védekeznünk azonban kell, hiszen mint tudjuk: attól, hogy valaki üldözési mániában szenved, még nem biztos, hogy nem akarják tényleg elkapni.

Kazári Csaba
felelős szerkesztő

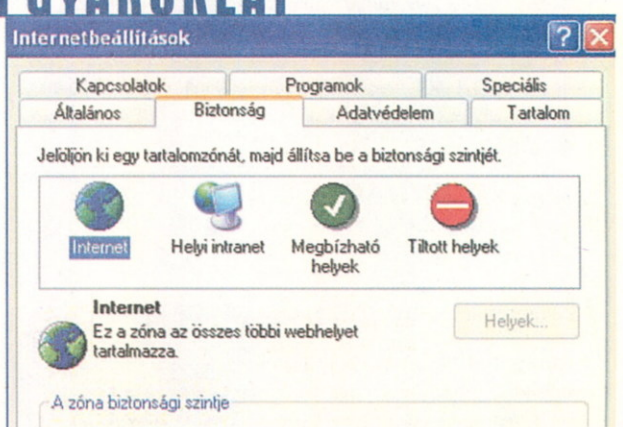
KÖRKÉP



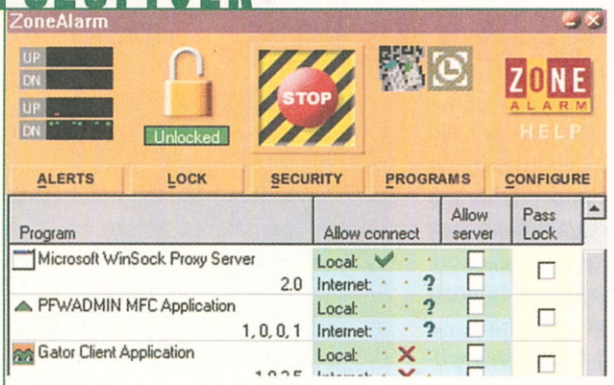
INTERNET



GYAKORLAT

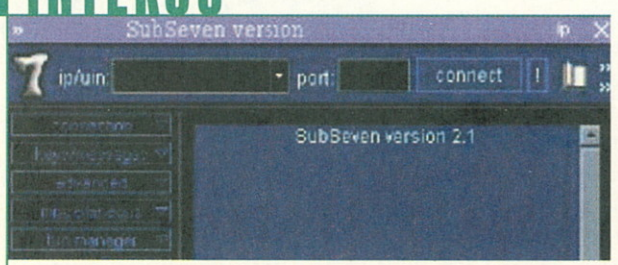


SZOFTVER



FÓKUSZ

INTERJÚ



Jelszavak feltörése 22

Az egyik legnagyobb akadályt változatlanul az okos jelszavas védelem jelenti a hackereknek, mivel az interneten és a helyi számítógépeken is gyakran védik ilyen titkos kifejezések a fájlokat és a postafiókokat a jogosulatlan hozzáférések ellen. Azonban mint tudjuk: minden feltörhető…

Az internet réseinek tömítése 27

A biztonsági szoftverek gyártói rendszeresen figyelmeztetnek az interneten villámgyorsan terjedő új szoftverekre. Időközben számos piackutató intézet felfedezte, hogy ennek ellenére bűnösen elhanyagolják a biztonság kérdését a magánhálózatokon és a számítógépeken. Pedig az interneten leselkedő veszélyek ellen nem is olyan nehéz védekezni. A nagyobb online biztonsághoz vezető út első lépései az aktuális böngészőverziók és patch-ek, a megfelelő programbeállítások és a hálón való ésszerű viselkedés.

Tűzfalak feltörése 37

A PC-nk egy tűzfal alkalmazásával még nem válik biztonságossá (ami persze egyáltalán nem jelenti azt, hogy a tűzfal felesleges lenne). Ennek két oka is van. Az egyik, hogy a tűzfal csak bizonyos veszélyek ellen képes védelmet nyújtani, a másik pedig, hogy a tűzfal is kicselezhető.

Bankkártyák, hitelkártyák, chipkártyák 40

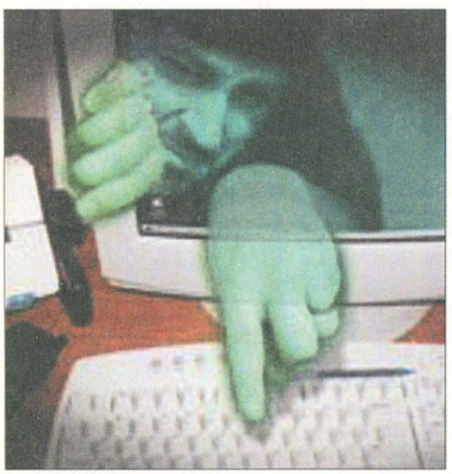
A hitelkártyák és a különböző mágnescsíkos kártyák, illetve chipkártyák pénzt helyettesítő eszközök, ezért a hamisításukra épp olyan nagy a kísértés, ha ugyan nem nagyobb, mint a pénz esetében. Ugyanakkor azt is el kell ismernünk, hogy a legtöbb kártya hamisítása nem igazán nehéz feladat. A bankok Magyarországon is számolnak a kártyacsalás kockázatával, együttműködésük következtében azonban ez a kockázat még elviselhető.

Ki kicsoda?

Az első és legfontosabb kérdés, hogy mikor is beszélünk hackerekről és crackerekről, mi a különbség közöttük, és egyáltalán, mivel is foglalkoznak valójában ezek a „speciális szakemberek".

Hacker

A *hacker* az angol *hack* igéből származó kifejezés, az eredeti jelentése: ácsolni, barkácsolni, míg a szó átvitt értelmű jelentése „kódfaragó". Az elnevezés az 50-es évekből származik, s a MIT nagygépeket programozó végzős diákok és szakemberek kezdték így nevezni magukat, mégpedig azért, mert az akkori gépek korlátaival találkozva (nagyon kevés memória volt a számítógépekben) megpróbálták minél kisebbre „összenyomni" a



Vajon ő egy hacker vagy cracker?

programokat és az operációs rendszereket. Belenyúltak tehát a programokba, rendszerekbe, illetve átírták azokat. Tették ezt mindenféle felhatalmazás nélkül, az optimális működés érdekében. Természetesen a programot nem változtatták meg, az továbbra is ugyanúgy működött, mint addig, csak jobban és kevesebb helyet foglalt. Minél sikeresebben faragott le valaki a kódból, annál nagyobb elismerés járt neki. Később a hacker kultúra némiképp átalakult, manapság a szó helyes értelmezése szerint: olyan „kimagasló számítástechnikai tudással bíró személy", aki szigorúan segítő jelleggel (tehát nem ártó szándékkal - ez nagyon fontos!) feltárja a számítógépes rendszerek/alkalmazások előnyeit és hibáit, illetőleg javít azokon. Sajnos a média a számítógépes bűnöző (betörő) szinonimájaként használja a hacker szót – helytelenül! Maguk a hackerek *script kiddie-nek, cracker-nek* vagy *exploitboy*-nak nevezik az ártó szándékú (honlapok feltörése, jelszavak ellopásávsl stv. foglalkozó) embereket, és élesen elhatárolódnak tőlük.

Hacker-közösségekből, -csapatokból elég sok van – általában a neten tartják a kapcsolatot egymással, de előfordul hogy hacker-találkozókat szerveznek, ahol személyesen is megismerhetik egymást. Az Egyesült Államokban és Nyugat-Európában 15-25 éves fiatalokból szerveződnek a hacker-csoportok, ilyen plddául a holland *Hack-tic*, az amerikai *Legion of Doom (LoD), a Masters of Deception (MoD), a Cult of the Dead Cow (cDc)* – hogy csak a „legismertebbbeket" említsük. A hacker-csoportokon belül a tagok mindegyike külön szakterületre szakosodik.

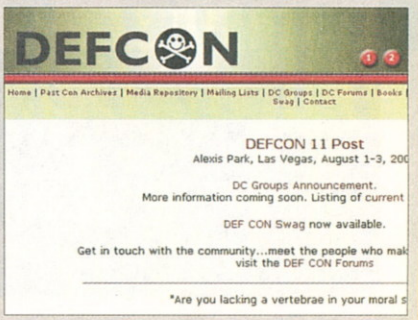
Cracker

A *cracker* szó a *to crack* (magyarul „törni") igére vezethető vissza. Elsődleges jelentése szerint olyan kárt okozó személy, aki számítógépes rendszereket rongál, illetve adatokat tulajdonít el vagy bármilyen egyéb módon kárt okoz. Ebben az értelemben többnyire maguk a hackerek, illetve néha a média használja ezt a szót. Másodlagos jelentése szerint (és ez az elterjedtebb): a cracker olyan valaki, aki a kereskedelmi forgalomban lévő szoftverek kódját megváltoztatja (s ez már önmagában egy illegális tevékenység) annak érdekében, hogy a szóban forgó szoftver szabadon másolható, használható és terjeszthető legyen. A programfeltörés a Commodore 64-es számítógépek megjelenésével egy időben kezdődött, a szó szoros értelmében vett (manapság is működő) PC-s „crackerkedés" azonban később, 1986-87-ben indult. A hackerkultúrával ellentétben, amely inkább cyberpunk jellegű laza közeg, a cracker világ igen összetartó és szerteágazó nemzetközi közösség: az Egyesült Államokban, Európában, Kínában stb. mindenütt vannak „csapataik". Persze ezek a teamek nemcsak a crackerekből, hanem a velük együtt dolgozó csapattagokból állnak: az eredeti program megszerzőitől a feltört programot terjesztőkig. Általában csak a hecc kedvéért dolgoznak, a nagyobb cracker-csapatok azonban igen komoly összegeket keresnek illegális tevékenységükkel, azaz a szoftverek feltörésével, terjesztésével. A csapatok között nagyon nagy a versengés, főleg a fejlettebb országokban, ahol a „warez-scene", azaz a cracker-csapatok és tevékenységük évtizedes hagyománnyal bír. Meglepő módon a magyar „warez-scene" is elég jelentős, többnyire azonban non-profit mó-

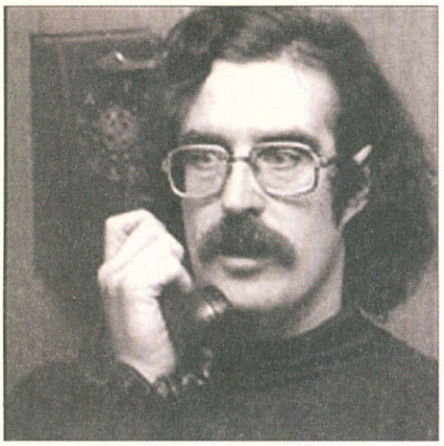
Hacker-konferenciák

A hackerek konferenciákat is szerveznek (DefCon, HoHoCon, H.O.P.E.-Hackers on Planeth Earth), ahol személyesen is találkozhatnak. Általában saját pólót nyomtatnak az esemény alkalmából, jellegzetes feliratokkal, például: *Root is a state of mind – Root-nak lenni (a Unixos gépek korlátlan hatalmú adminisztrátora) egy szellemi állapot.* Vagy: *Why? Because We Can! – Hogy miért tesszük? Mert képesek vagyunk rá!*

Az FBI természetesen tud a konferenciákról, és képviseltetik is magukat, amire a résztvevő hackerek egy mára hagyományossá vált, „mókás" *Spot the FEDs* (Szúrd ki az ügynököt!) névre hallgató vetélkedővel válaszolnak.



A hackerek konferenciákat is szerveznek, ahol személyesen is találkozhatnak



„Captain Crunch", az egyik leghíresebb phreaker

don és relatíve „kicsiben" működik. Az igazi magas szintű cracker-csapatokba igen nehéz bekerülni, a crackerek nem igazán „barátkozó" típusok. Igazából négy-öt igazi „nagy" cracker-csapat van a világon (pl. a híres *Elite* vagy a *Myth*) és persze sok-sok kisebb.

És a többiek...

Hogy a helyzet ne legyen túl egyszerű, a sajtó, illetve maguk a hackerek is többféle kategóriát használnak még a fentieken kívül.

Phreaker. (a „phone phreak" szóból). A phreaker-ek a telekommunikáció szakértői, „átprogramoznak" távközlési berendezéseket, ingyen mobiltelefonálnak és interneteznek (vonalat „lopnak"), értenek a lehallgatáshoz, a mobiltelefonok kikódolásához, átprogramozásához, titkosításához stb.

Mivel csak a kommunikációs eszközök és hálózatok „törésével" foglalkoznak, külön kategóriát képviselnek. Magyarországon még kialakulóban van a phreaker tevékenység, azonban a „phreaker-scene" szülőhazájában, Amerikában (hol is máshol?), majdnem ugyanakkora közösséget alkotnak, mint a hackerek. Az első és leghíresebb phreaker (neki tulajdonítják az elnevezést is) *Stewart Nelson* volt, aki 1964-ben rávette az akkori nagyszámítógépeket, hogy egy kis „frekvenciagenerálás" segítségével ingyen távolsági hívásokat bonyolíthasson. A phreaker scene leghíresebb tagja *Joe The Whistler* volt (még 1969-ben). Joe vakon született, viszont megvolt az a különleges képessége, hogy tökéletes 2600 Hz-es hangot „fütyült" (innen származik a neve). A 2600 Hz-es hang az úgynevezett „in-band" jelzés, amely a távolsági hívást, azaz a „long-distance-call"-t kezdeményezi a központ felé az Egyesült Államokban. Ezzel a nem mindennapi tudással Joe gyakorlatilag ingyen tudott távolsági hívásokat bonyolítani, a telefontársaságok nagy bánatára. Manapság a phreakerek a mobiltelefonok kikódolásával és mobilhálózatok törésével és „buherálásával" foglalkoznak, s a 2600 Hz-es jelet sem „fütyörészik", hanem egy kis szerkezettel (Blue-Box) állítják elő.

HPAV (a Hacking, Phreaking, Anarchy, Virus szavakból). Ez a tevékenységi kör nem sorolható sem az egyik, sem a másik oldalra – szerencsénkre Európában gyakorlatilag nem létezik, Amerikában azonban igen erősen jelen van. A HPAV csapatok a létező legkártékonyabbak: vírusokat írnak, állami szervek munkáját teszik tönkre, magánszámítógépekbe törnek be, mindezt csak azért, hogy másoknak gondot okozzanak.

A HPAV kifejezés egyébként azért terjedt el, mert sem a hackerek, sem a crackerek nem vállalnak közösséget ezekkel az emberekkel – kitaláltak hát egy külön elnevezést nekik. A HPAV scene tagjai a szó szoros értelmében vett számítógépes bűnözők (ezúttal idézőjel nélkül !), legismertebb képviselőik a vírusokat író (pl. Red Code, Slammer) programozók és csapatok.

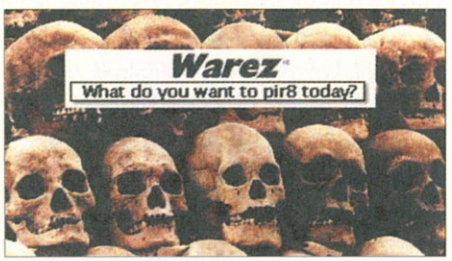
Script-kiddie. Se nem ez, se nem az – nem túlzottan nagy tudású számítógép-buherátorok, akik főleg hírnévre vágyakozva és a „ki ha én nem" mentalitás miatt, kisebb balhékat csinálnak – főleg defacement-eket, azaz honlapok feltörését és megváltoztatását. Nem tartoznak a hackerek közé (ők nem csinálnak rosszat, ugyebár), viszont nincsen akkora tudásuk és annyi kárt sem okoznak, hogy crackerek lennének – ezért két szék közé esve, ebbe a kategóriába kerültek. A nagyközönség és a média persze őket is hackernek nevezi. A hackerek közéjük sorolják például az Elender vagy a BRFK honlapjának feltörőit is – csak hogy magyar példákat is említsünk. ■

Egy kis warez-történelem

Hogyan kezdődött?

Ahogy napvilágot láttak az első számítógépek, illetve szoftverek, a szoftverkalózkodás is azonnal megjelent – bár a kezdeti időkben még nem hackerekről, crackerekről és warezről beszélték, hanem egyszerűen csak „pirates", azaz kalózok volt az elnevezés. Ha egy programot megírnak, mindig lesznek, akik azt ezer részre szedik és „felboncolják" – s ez valószínűleg így is lesz, amíg csak világ a világ…

A kalózkodás a 80-as (egyes források szerint a 70-es) években indult, viszont a megszületése után rögtön elképesztő méreteket öltött (nem kicsiben kezdték!) Az Európában forgalmazott korai *BBC-Macro* számítógépekre írt szoftvereket például olyannyira „feltörögették", hogy pár év múlva az akkori szoftvercégek egész egyszerűen már nem fejlesztettek erre a platformra: nem érte meg ugyanis programokat írni, mert gyakorlatilag egyetlen fillér bevételük sem volt a kalózok miatt.



Az úgynevezett warez-scene kialakulása (azaz, amikor a crackerek elkezdtek csapatokba szerveződni és összehangoltan dolgozni) 1978-79-re tehető: az Apple II gépek idejében alakultak meg az első kalózcsoportok. 1981-től körülbelül 1987-ig a mai értelemben vett PC még nem volt egyeduralkodó, a kalózkodás fénykora tehát a Commodore gépek idejére tehető. Ekkor alakultak ki a ma is használatos eljárások, csapatok és maga a warez-kultúra is. Fiatal srácok foglalkoztak a törésekkel – eleinte jó bulinak tűnt, hogy a „másolhatatlan" gyári szoftvert feltörik, és továbbadják a haveroknak, később azonban kiderült, hogy ezzel keresni is lehet.

A programok feltörése nem volt túl nehéz a hőskorban: általában valamilyen egyszerű másolásvédelmet raktak a játékokba, néha pedig magára a gyári flopilemezre. A feltört szoftverek azután fénysebességgel terjedtek; először csak azon a környéken ahol a cracker lakott, ám a BBS-ek és a modemek megjelenésével már az egész világon. Volt, aki pénzért, és volt, aki ingyen és szórakozásból crackelt – mivel azonban a Commodore gépekre rengeteg szoftver készült, a helyzet áttekinthetetlen kezdett lenni. Sokan nem is „szerveződtek", és nem is léptek be semmilyen csapatba, csak magányosan dolgoztak. A feltört programot, illetve – mivel többféle törés is van – a törés verzióját néha csak arról lehetett megismerni, hogy a cracker egy pici „credit"-et helyezett el a nevével, a képernyő sarkában (pl. „Cracked by Nomade").

Volt, hogy egy programot százan is feltörtek a világ különböző részein, még más szoftverek valahogy kimaradtak. Muszáj volt valahogy rendbe tenni a dolgokat. A kapcsolattartás és a szerveződés azonban nehézkes volt, mivel az akkori BBS rendszerek lassúak, drágák és megbízhatatlanok voltak. Egy egyszerű fiatal cracker nem engedhette meg magának, hogy komoly pénzekért BBS-eken keresztül töltse fel a szoftvereket és tartsa a kapcsolatot társaival. Persze a hackerek mindenütt jelen vannak – a warez-scene kialakulását is egy hacker, egész pontosan egy *phreaker csapat*, a *NAP/PA* jegyezte…

A BBS és a courier-ek

Az első BBS a hetvenes évek végén indult Apple II számítógépeken. Egy BBS-t már akkoriban is sok mindenre bevetettek, a leghasznosabb tulajdonsága azon-

A leghíresebb warez BBS a 80-as évekből: a Park Central

Ördögi színpad?

Az angol *scene* szó jelentése: színhely, színtér, színpad. A *warez-scene* nem is annyira szó, mint inkább egy jelenség. Sajnos mindezidáig nem sikerült rá tökéletes magyar megfelelőt találni, így a magyar PC-s szlengben is a „szkéne" elnevezést használják. Ellentétben a hackerekkel, a warez-csapatok (élükön a crackerekkel) szoros, szinte katonai felépítésű egységekben működnek – magányos cracker tehát nem létezik. (Érthető, hiszen ha valaki kiszedi a másolásvédelmet egy programból, az még nem vezet sehova: szükség van valakire, aki összetömöríti, majd terjeszti azt és így tovább). Minden cracker egy csapat tagja – a csapatok hangzatos fantázianeveken azonosítják magukat, és általában elég erős versengés van közöttük. A csapatok összessége a warez-scene.

Érdekességek

„A mai technológiával nincsen száz százalékos biztonságot nyújtó mód a kalózkodás bármely formájának a megállítására. [...] Bizonyos idő alatt egy jó cracker fel tud törni bármilyen védelmet – ez a szoftver sajnálatos velejárója..." – *James Summers (Activision – ZED/1999)*

„Nagyon fontos, hogy megvédjük a piacot a kalózmásolatoktól, mert (habár a játékosok számára jó üzletnek tűnik a beszerzésük) gyakran hibásak, nem teljesek, nem nyújtják ugyanazt a játékélményt, mint az eredeti program – ez pedig nemcsak anyagilag káros nekünk, hanem a jó hírünket is rombolja..." – *Simon Maflin (GT Interactive – ZED/1999)*

Magyarországon megközelítőleg 50 ezren játszanak rendszeresen valamilyen játékkal PC-n vagy Playstation-ön. A magyar forgalmazók kimutatásai szerint egy játékból átlagosan 2-3000 példány talál gazdára a boltokban.

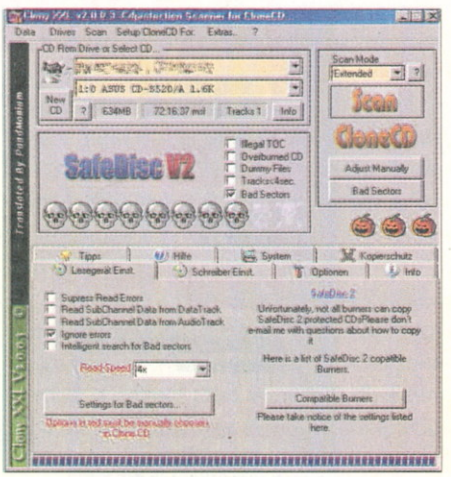
ban a fájlátvitel volt: a korai BBS-ek tömkelegével tartalmaztak feltört szoftvereket. Az internettel ellentétben azonban, a BBS használata nagyon drága volt – egy-egy komolyabb programcsere érdekében távolsági, sőt nemzetközi hívásokat kellett bonyolítani. A warez-scene tehát már kialakulóban volt, a programok gyors elterjedése azonban nagyon lassan történt. A crackerek nagyon értettek a szoftverek feltöréséhez, a phreakerek viszont tudták a módját a BBS rendszerek ingyenes vagy olcsó használatának. Az egyetlen probléma az volt, hogy nem voltak jóban... egészen 1988-ig. Ekkor alakult meg ugyanis a *North American Pirate Phreak Alliance (NAP/PA)* nevű hacker/phreaker csapat – ők készítették a *How To's of Phreaking for the pirates* című remekművet, amelyet azután villámgyorsan el is terjesztettek a BBS rendszereken. A későbbiekben is segítettek a crackereknek abban, hogy ingyen vagy olcsón tudják használni a drága BBS rendszereket. (Hogy miért tették mindezt, arra rengeteg magyarázat van, de egyik forrás sem állít biztosat – szóval a motiváció a múltba veszett).

Elhárult tehát az első akadály – a BBS-ek használata és a nagy (akkoriban a 30K is nagynak számított) fájlok cseréje sem okozott gondot a crackereknek. Elindult a BBS-ezés, majd később az internetezés, semmi sem állhatta útját a mai warez-világ kialakulásának. Persze a nagy szoftverkiadók és -fejlesztők sem nézték tétlenül, hogy ilyen szervezettséggel működjenek a szoftverkalózok, elkezdődött tehát a warez-háború.

Virtuális háború

Mint talán az eddigiekből is kiderült, a kalózkodás egyidős az első személyi számítógépekkel, a ZX-Spectrumokkal és a Commodore 64-esekkel. (Az első számítógépes játék a világon a *Space Wars* volt, s valószínűleg csak azért nem törték fel, mert a futtatásához egy kisebb tornatermet elfoglaló, akkoriban „szuperszámítógépnek" számító masina kellett.) A szoftverfejlesztő cégek eleinte egyáltalán nem foglalkoztak az illegális másolatokkal, pár fiatal hobbijának tekintettek csupán a töréseket és a szoftverkazetta cserélgetéseket, egészen addig, amíg meg nem jelentek az első flopiegységek a C64 és az Apple gépekre. A lemezmeghajtókkal ugyanis nagyon könnyen és viszonylag gyorsan lehetett nagy mennyiségben is másolni. Érdekes módon a cégek rengeteget vesztettek a kalózkodáson, ugyanakkor a hardveresek óriási összegeket kerestek – a C64-es gépeket szinte kizárólag játék céljára vásárolták akkoriban, játék pedig, a crackerek jóvoltából, bőven volt.

Persze eljött az idő, amikor a szoftvercégek már annyit vesztettek a kalózkodás elterjedése miatt, hogy kénytelenek voltak cselekedni: bebizonyosodott, hogy a másolgatás nem pár fiatal hobbija, hanem szervezett és az üzletet veszélyeztető tevékenység. (Németországban a 80-as években egy a tízhez volt az eredeti és az illegálisan másolt szoftverek aránya...) Az első hibás lépést a 80-as évek végén követték el a szoftveresek: az illegális másolgatás elleni védekezésül felemelték programjaik árát, gondolván, hogy így kevesebb eladott termékből is nyereséget tudnak produkálni. Az ötlet olyan „csodálatos" volt, hogy hatására az addig becsületes, a boltokban vásárlók is áttértek az illegális programmásolgatásra, a warez tevékenység a csúcsára érkezett... Az áremelés tehát nem vált be, s ezt felismervén kezdtek el a cégek egyszerűbb-bonyolultabb védelmi eljárásokat építeni a programjaikba. A hatás nem is maradt el, megjelentek a crackerek, és a történet innentől már ismert.



„Feltört szoftverek – minden mennyiségben"

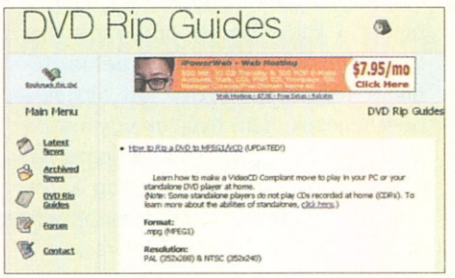
Clone CD – nemcsak bárányt, CD-t is lehet klónozni

Bármilyen meglepő, még a törvény is a crackerek oldalán állt: az akkoriban hatályos jogszabályok szerint ugyanis, ha valaki (például maga a cracker) legálisan megvásárolta a szoftvert, az onnantól az ő tulajdonát képezi: gyakorlatilag tehát azt csinál vele, amit akar, még a szecskavágóba is beteheti. A crackerek tehát nyugodtan babrálhattak a kóddal, ízekre szedhették a szoftvereket – semmi sem állíthatta meg őket. A 80-as évek második felére a szoftvergyártók kifújtak az ötletekből, látszólag feladták a harcot...

Ekkoriban jelentek meg a crackereket és a vásárlókat összekötő ügyes és élelmes „üzletemberek" is, akik újsághirdetésekben árulták a másolt szoftvereket, a nagyobb másolópartikon (copy-party) pedig nemritkán több száz fiatal adta-vedte a gyárinak igazán nem nevezhető szoftverpéldányokat. Már-már úgy tűnt, hogy a kalózkodásnak semmi sem állhatja útját, amikor a gyártók ismét ellentámadásba

lendültek: a 90-es évek elején megjelent a piacon a CD-ROM.

A CD-lemezek bevezetésével a fejlesztőcégek nyugodtan hátradőlhettek: a CD-n forgalmazott játékokat nehézkes (vagy lehetetlen) volt flopira másolni, a CD mint adathordozó új védelmi eljárásokat tett lehetővé – úgy tűnt, hogy leáldozott a warez-világnak. Persze a sors közbeszólt: a hardvergyártó cégek ugyanis nem hagyhattak ki egy ilyen esélyt a piacon: megje-



Sokáig a DVD tűnt biztos védelemnek. De nem túl sokáig...

lentek a CD-írók és a viszonylag olcsó írható CD-lemezek is. A kalózok tehát visszavágtak, bár nem úgy, ahogyan az várható volt: kiderült, hogy a CD-lemez kétélű fegyver... A crackerek ugyanis ahelyett, hogy a gyári CD-lemezt egy az egyben lemásolták volna, kitalálák a *rip*-et, azaz a „lecsupaszított" szoftvert: ezáltal az eredeti, az egész CD-t elfoglaló játék helyett akár 50 db játék és egyéb szoftver is elfért egyetlen írható lemezre, persze gondosan összecsomagolva (akkoriban a szoftverek terjedelme 10 és 200 Mbájt körül mozgott).

A történelem tehát itt is megismételte önmagát: a warez újfent virágzott, a szoftvergyártó cégek ismét hatalmasat „buktak", a hardveresek pedig megint csak jól jártak: az emberek úgy vitték az írható CD-lemezt és a CD-írókat, mint a cukrot. A nagy cégek persze most sem tanultak a hibáikból: ahelyett, hogy termékeik árának csökkentésével próbálnák meg ösztönözni a legális piacot, az árakat folyamatosan magasan tartják – napjainkban a DVD-lemezektől várják az áttörést, azaz a kalózkodás visszaszorítását. Persze DVD-író és írható DVD-lemez is létezik, szóval sejteni lehet a jövőt ....

A warez-háború manapság is zajlik: az egyik oldalon multinacionális óriáscégek állnak, szemben a láthatatlan és szervezett kalózokkal. S hogy végül ki lesz a győztes, azt majd az idő (s talán egy megfontoltabb üzletpolitika) dönti el. ■

Jogi esetek

Manapság senki sem vitatja, hogy szükség van a szoftvereket érintő törvényi szabályozásra. Sajnos ez a szabályozás nem teljesen kiforrott, mi több, amint az cikkünkből is kiderül, meglehetősen sok benne a homályos folt.

Egy hazai eset

A Budai Központi Kerületi Bíróság 2002. március 05. napján hozott jogerős ítéletet *Herpai Gergely* ügyében, aki *Costello* néven illegális szoftvereket értékesített az interneten keresztül. Három rendbeli jelentős vagyoni hátrányt és 1339 rendbeli üzletszerű, részben folytatólagosan elkövetett szerzői vagy szomszédos jogok megsértése bűntette miatt a vádlottat a Bíróság 8 hónapi börtönbüntetésre ítélte, aminek a végrehajtását 2 év próbaidőre felfüggesztette.

Új bűnözési formák?

A számítógépek elterjedésével a bűnözésben több szempontból is új dimenziók nyíltak. *August Bequai* washingtoni professzor az Európa Tanács Miniszteri Bizottsága 1989. szeptember 13-án megjelentetett, 1989. évi 9. számú Ajánlásának bevezetőjében az alábbiakat írja:

„A számítógép forradalma együtt járt a visszaélések és a bűnözés új formáinak a kialakulásával is. A világot átfogó számítógép-hálózatba tetszésük szerint, büntetlenül bekapcsolódhatnak arra illetéktelenek, műszaki etika, úgy tűnik, nem létezik, a modern bűnözők kihasználják a hatályos jogi rendszerek hézagait, és megmenekülnek a büntetőjogi felelősségre vonástól. A számítógép forradalma előállította azokat az eszközöket, amelyekkel büntetlenül lehet lopni, ellenőrizni, és manipulálni lehet milliók gondolatait és tevékenységét és az egész társadalmat túszul lehet ejteni." – *www.jogtar.hu*

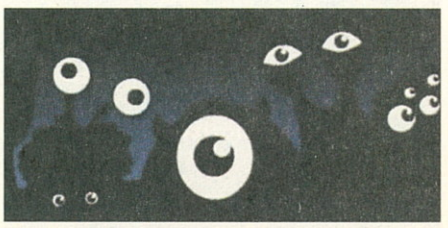
Bármilyen meglepő is, a törvényi szabályozásban jelenleg nincsen meghatározva a kártérítés mértéke. Ez pedig már csak azért is nehezíti meg a helyzetet, mert míg egy vadonatúj, a legkorszerűbb fejlesztéseket kamatoztató 3D-tervező szoftver értéke elérheti az egymillió forintot, addig egy tízéves játékszoftver (amelyet esetleg már a kereskedelmi forgalomból is kivontak) értéke gyakorlatilag a nullával egyenlő.

Jó szabály, rossz szabály?

Ennek ellenére a jogszabály nem tesz különbséget illegális szoftver és illegális szoftver között – elméletben tehát az is lehetséges, hogy valakit elítéljenek azért, mert egy több mint tízéves *Super Mariót* futtat a gépén – illegálisan. A valóságban persze nincsenek ilyen sarkított esetek (szerencsére), hiszen a törvény nem az otthoni felhasználók, hanem az illegális szoftverkereskedelmet folytatók ellen készült.

A szoftverhamisítás 1993. május 15-e óta a szerzői és szomszédos jogok megsértéséről szóló törvény körébe tartozik. A jogszabály szó szerint: *„Aki irodalmi, tudományos vagy művészeti alkotás szerzőjének [...] vagyoni hátrányt okoz, vétséget követ el, és két évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel büntethető."*

Mindannyian ismerünk történeteket,



A crackerek nem véletlenül láthatatlanok, hiszen a szabadságukat kockáztatják...

amikor illegális szoftverek birtoklásáért vagy terjesztéséért indítottak eljárást. Európában az első ilyen eset Csehországban történt: egy számítástechnikai üzlet vezetőjét és az ott dolgozó informatikust 2 hónap büntetésre vagy 300 dollár megfizetésére ítélték – és persze az okozott kárt (100 dollár) is ki kellett fizetniük. A mai esetek fényében az összegek elég jelentéktelennek tűnnek, de hát ez csak a kezdet volt.

2002-ben a BSA ötszámjegyű (!) jutalmat fizetett angol fontban annak az informátornak, aki feljelentette saját munkaadóját: a cégnél több mint 400 db licenc nélküli MS Office és Windows operációs rendszer futott.

Az eddigi legsúlyosabb ítéletet Görögországban várható: egy amerikai állampolgár honlapján árulta az illegális szoftvereket, s a büntetése akár *tíz év börtön* és *ötvenezer dolláros bírság* is lehet.

Tanulságos esetek...

Az első magyarországi eset (bár nem kapott túl nagy publicitást) még a C64-es korszakra datálódik: a Petőfi Csarnokban rendezett másolópartit (copy-party) árasztottak el a rendőrök, a résztvevő 12-16 éves fiatalok nem kis ijedtségére. Az ott talált számítógépeket lefoglalták, valamint több ezer lemezt és kazettát is elkoboztak – ezeket később bezúzták. Az esetnek akkor még nem volt jogi következménye.

Az első jogerős elmarasztaló ítéletre 1996-ban került sor: két soproni fiatalember saját BBS-t üzemeltetett, ahol számítógépes programok cseréjét tették lehetővé, de persze nem rendelkeztek ezen szoftverek a jogaival. Érdekesség, hogy a fiatalok mindezt anyagi ellenszolgáltatás

nélkül tették: a BBS üzemeltetése a hobbijuk volt. 250 és 150 nap börtönbüntetést kaptak, és jelentéktelen összegű kártérítést kellett fizetniük. No persze nem úsztak meg ennyivel: a perköltséget is nekik kellett állniuk, ami már közel sem volt olyan jelentéktelen (340 000 forint).

Egy másik, igen nagy nyilvánosságot kapott ügy 1997-ben történt: egy győri számítástechnikai cégről kiderült, hogy tevékenységi körükbe tartozik a nem kifejezetten legális szoftverek árusítása is – tizenkilenc cégvezető és alkalmazott ellen emeltek vádat. A megállapított kár harminchárom millió forint volt, tehát valószínűleg nem „kicsiben" űzték az ipart.

1999 elején történt a mindmáig legnagyobb port felverő eset, az azóta csak „pécsi vészként" emlegetett házkutatássorozat. A dolog némileg valóban „ízetlen" volt a hatóságok részéről: a nyomozók eljutottak egy nagyüzemben másoló kalózhoz, akinél 412 darab CD-t és egy címjegyzéket(!) találtak. A címjegyzékben mindazoknak a neve szerepelt, akikkel a kalóz már üzletelt. Ez eddig még nem is lett volna probléma (hiszen a kalózkodás valóban nem szép dolog), viszont a nyomozást vezető századosnő utasítása alapján a rendőrök a címjegyzékben talált összes címre elballagtak, házkutatást tartottak és töménytelen mennyiségű CD-t, számítógépet (volt ahol monitort és szkennert(?) is) lefoglaltak. Természetesen a kilencvenegy „vádlott" szinte mindegyike iskolás vagy főiskolás/egyetemista volt, s némelyikük csak egy(!) darab másolt CD-vel rendelkezett. Az ügyben végül is nem szabtak ki börtönbüntetést. Szerencsére a „pécsi vész" elszigetelt esetnek mondható, s úgy tűnik, hogy mostanság a BSA és a rendőrség is az európai mintát követi: egész pontosan a terjesztőkre és az igazi kalózokra koncentrálnak, s nem zaklatják az otthoni felhasználókat.

A BSA nagy port felverő plakátja...

Az első ítélet...

2003 január 9-én megszületett ez első olyan ítélet, ahol jogosulatlan szoftver használatért egy év letöltendő(!) börtönbüntetést szabtak ki. *Vámosi Zsolt*, a Philos Labs. játékfejlesztő cég korábbi vezetője volt a vádlott, az ítélet vegyes érzelmeket kavart a számítástechnika szerelmeseinek körében, hiszen Vámosi annak ellenére kapta a büntetést, hogy az okozott kárt teljes egészében megtérítette.

Jó tudni...

Végül nem árt tisztában lennünk azzal, hogy mi minősül illegális szoftverhasználatnak:

– Végfelhasználói túlhasználat (például ha van egy legális Windowsunk, de ugyanazt a példányt feltelepítjük a cégen belül vagy otthon több számítógépre is).

– A kereskedő az eladásra szánt, összeállított gép merevlemezére másolja a programot (például a boltban „felraknak" nekünk egy Windowst és egy-két játékot).

– A hamisítás (az eredetivel teljesen megegyező megjelenésű másolat).

– Az internetről letöltött illegális szoftverek (itt elég homályos a határvonal, hiszen honnan is tudhatnánk, hogy amit letöltünk az illegális-e avagy sem).

A BSA mint a szoftvergyártók érdekképviseletében eljáró szerv feladata persze nem az, hogy mindenkit börtönbe zárjon, aki nem regisztrálta a WinZIP-et a nyári konyhában üzemelő 486-os gépen. A kezdeti lelkes „túlkapások" után nem is találkozhatunk olyan precedenssel, ahol „melléfogásról", esetleg eltúlzott büntetésről van szó. Kivételt képez ez alól az elhíresült Vámosi féle eljárás (lásd keretes írásunkat) – persze ennek a megítélése némiképp szubjektív. Egy a lényeg: figyeljünk arra, hogy ne használjunk illegális szoftvert, és akkor nem lehet gond. ■

Cracker módszerek

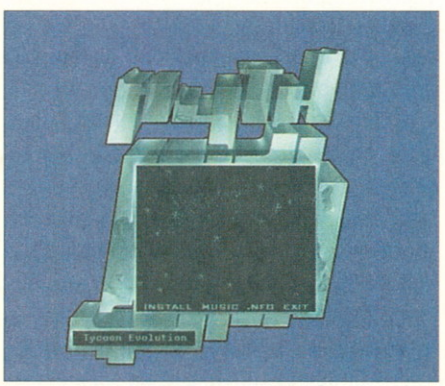
Egy olyan szoftvert működésre bírni, amelyet nem a boltban vásároltunk, sok esetben nem könnyű. A crackerek persze igyekeznek automatikus és „felhasználóbarát" módszereket találni. A legjobban elterjedt megoldások: a crack.exe, a szériaszám-generátor (keygen), a javítófájl (patch), illetve a szériaszám (serial).

Crack

Leginkább a játékszoftverek esetében használják ezt a megoldást – az illegális és a gyári verzió teljesen ugyanaz. Az egyetlen különbség, hogy a warez-példány egy *crack.exe-t* is tartalmaz (ez persze lehet egy „akármi".exe is). A szoftver futtatható részét (pl. játékprogram.exe) telepítés után a crack.exe felülírja (vagy automatikusan, vagy nekünk kell rámásolni) – és máris használható a program, mindenféle regisztrálás, regisztrációs szám és egyéb műveletek nélkül. Az eljárás nagyon egyszerű: az eredeti futtatható fájlból emelik ki azon részeket, amelyek a regisztrációt vagy a másolásvédelmet végzik – a játék.exe-ből így lesz crack.exe. Mindkettő ugyanaz, csak az utóbbi pár bájttal kisebb és teljesen ingyenes... A nagyon profi és „előzékeny" warez-csapatok, saját installert írnak, és automatikusan feltelepítik a crack-et – így a felhasználó semmit sem észlel a folyamatból.

Szériaszámok minden mennyiségben...

Egy szériaszám-generátor



Egy warez installer – mi tagadás, jobban mutat, mintha „gyári" lenne

Mit mond a hacker?

„... néha előfordul, hogy a készítők egyéb védelmi algoritmusokat is raknak a programba, amire nem számítunk. Pl. ha ismered a *Settlers* nevű játékot, akkor tudod, hogy hiába törték fel, egy idő után a program felismerte, hogy nem gyári CD-ről fut, és a játékban a kovácsműhely fegyverek helyett malacokat kezdett gyártani..."

Szériaszám-generátor (keygen)

Főleg irodai alkalmazások, illetve 30 napos, limitált, úgynevezett próbaverziók törésére használt eljárás. A limitált verziójú szoftverek vagy időkorlátosak (általában 30 nap vagy X számú elindítás) vagy funkciólimitáltak (például minden működik, de nem lehet a munkát elmenteni stb.). Ezeket a limitált szoftvereket felesleges feltörni, jóval egyszerűbb egy szériaszámot generálni. Ha e számot megadják, a szoftver úgy érzékeli, hogy regisztrálták (azaz megvették), és máris megszűnnek a korlátozások. A *keygen-ek* matematikai modell alapján működnek, a cracker a szoftver szériaszám-ellenőrző rutinjának alapján állítja elő a képletet, amellyel azután valós regisztrációs számokat tud generálni.

Patch

A mindennapi számítástechnikából is ismert javítófájlt a crackerek is előszeretettel használják. Nem ritka, hogy a törés után a szoftver mégsem működik megfelelően (a crackernek nem az a dolga, hogy minden feltört játékot végigjátsszon, ugyebár...), ilyenkor a warez-csapatok javítófájlokat publikálnak, ami rendbe hozza a hibát.

Serial

Egy szoftver illegális terjesztésének a legegyszerűbb módja, ha valakitől, akinek „gyári verziója" van, elkérjük a regisztrációs kódot. Ez persze nem egyszerű, de nincs is rá szükség. Az egyszerűbb szoftverek esetében a cracker csak egy NFO fájlt csomagol a program mellé, benne a regisztrációs számmal – ezt a számot bepötyögve, máris teljes értékű felhasználók leszünk. Néhány program esetében egyszerűen kiveszik a regisztrációra vonatkozó részeket – a regisztrációs mezőbe bármilyen számot vagy nevet beírhatunk...

Az itt is ismertetett alapvető eljárásokon felül persze még többféle törési mechanizmus is létezik: a crackerek kreativitása nem ismer határokat... ■

Kevin Mitnick

Kevin Mitnick – most éppen nincs letartóztatva

Kevin David Mitnick valószínűleg nem a világ legnagyobb és legjobb hackere – azonban kétségtelen, hogy ő a leghíresebb. Számtalan könyv és film dolgozta fel az életét és munkásságát. A könyvek közül a leghírhedtebb a „The Art of Description (A megtévesztés művészete)" című, amelyet maga Mitnick írt.

Amikor a hóhért akasztják

2003 februárjában a világ legismertebb hackerének abban a megaláztatásban kellett részesülnie, hogy feltörték biztonsági tanácsadással foglalkozó cégének weboldalát. Kevin Mitnick meglehetősen zavarónak tartotta az eseményt, de nem elég komolynak ahhoz, hogy hívja az FBI-t. Egy önmagát *BugBear*-nek nevező hacker egy oldalt adott hozzá Mitnick vállalati honlapjához, amelyen üdvözölte a sztárhackert, valamint elmondta: öröm volt betörni a „dobozába".

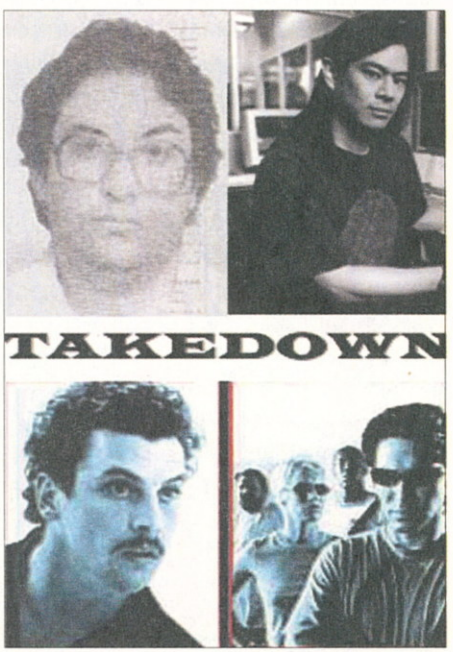
Érdekes nyilatkozatok Kevintől

„Igen, a hackerek egy megfelelően koordinált csapata le tudná rombolni a kommunikációs rendszereket, az energiahálózatot és talán a pénzügyi piacot is. De mindezen rendszerek igen hamar magukhoz térnének, lehetetlenség hosszabb ideig kiiktatni őket."

„Mindenki csodálkozott is, hogy nálam voltak a hitelkártya-adatok, és mégsem használtam fel azokat anyagi haszonszerzés reményében, és hogy sosem értékesítettem a kártyaszámokat."

„Valóban, programozói tudásom nem verdesi az eget. Inkább az emberek agyát hackelem, semmint a kódokat. Ha meg kellene tudnom egy szupertitkos adatot, előbb kezdenék el kutakodni a cég biztonsági szakembereinek fájljai között, minthogy mindenféle kódokkal bajlódjak. Egyszerűen így sokkal hatékonyabb az egész."

Külföldön a *TakeDown* című életrajzi film képezi a Mitnick kultúra filmes alapját, míg Magyarországon a *Hackers 2* című filmből ismerhették meg a nézők Kevin életének egy szakaszát. Mitnick a Guiness Rekordok könyvének 1999-es kiadásában a *Most Notorious Computer Hacker* címet is elnyerte, sőt az Egyesült Államokban, a *The Druids* nevű zenekar jóvoltából, egy sláger is született, *Free Kevin* címmel. Hírneve ellenére Mitnick nem mondható anyagias hackernek, bár az általa ellopott szoftverek értékét (a betörésekből származó károkkal együtt) több százmillió dollára becsülik, a hackert mégis mindig kirendelt védőügyvéd képviselte – s bármilyen meglepő is, mindig pénzhiányból kifolyólag.



Kevin és üldözője a valóságban és a filmvásznon

A világ legnagyobb (?) hackere

Kevin azonban inkább mítosz, mint igazi hacker, rengeteg fórumon, könyvben és üzenőtáblán olvashatjuk, hogy a tudását tekintve inkább csak amolyan „hackerecske", viszont a média és a sajtó kultuszt generált belőle. Így lett szegény Kevin Mitnick a világ leghírhedtebb és legveszélyesebb számítógépes zsenije.

A Mitnick körüli hisztériát jól példázza, hogy miután elfogták és öt év börtönre ítélték, a hatóságok annyira féltek, hogy világháborút fog kirobbantani, illetve összeroppantja a tőzsdét és az elektronikus kereskedelmet, hogy a büntetése alatt (sőt még utána!) sem kerülhetett mobiltelefon, számítógép vagy egyéb kommunikációs eszköz közelébe.

De vajon miért ez az óriási hisztéria? Hogy tökéletesen megértsük a Mitnick-kultuszt, mindenel előtt meg kell ismernünk közelebbről is Kevin életútját, elkövetett „csínyeit", motivációit. És persze gondolnunk kell az amerikai átlagember tájékozatlanságára is.

Cél: a telefonközpont

A telefonközpont manipulálásának több módja van, a leggyakoribb a *bounce* vagy a *hops* eljárás: a hacker több központon és telefonszámon át éri el a célt, miközben folyamatosan változtatja ezt az útvonalat. Így elég nehéz bemérni a hívást, a 80-as években pedig szinte lehetetlen volt.

A kis Kevin

Az igazság elkeserítő: Kevin Mitnickben nincsen semmi „különleges". 1964-ben született, és Los Angeles jómódú külvárosában nőtt fel. Szülei igazi középosztálybeli amerikaiak voltak. A 70-es években elindult a robbanásszerű informatikai fejlődés, Kevin pedig – mint szinte minden fiatal akkoriban – a számítástechnika rabja lett. Eleinte a telekommunikáció nyűgözte le – a telefonok és a modemes kapcsolat korában ez érthető is volt. Ez idő tájt alakult ki az *Underground Phreaker Scene*, akkoriban ugyanis még nem igazán voltak hackerek, inkább csak phreakerek. Természetesen Kevin sem maradhatott ki a divatos „telefonáljunk ingyen" játékból: egy számítógép és egy modem segítségével a digitális telefonközpontot babrálták barátaival, s ingyen telefonáltak, sőt belehallgattak mások beszélgetéseibe. Nem sok idő kellett hozzá, hogy az egyik phreaker csapathoz csatlakozzon. Rendszeresen találkozgattak egy pizzériában; itt szőtték világrengető terveiket és osztották meg egymással a tudásukat. Kevin kis csapatának példaképe a korszak leghíresebb „telefon-buherátora", egy *John Draper* nevű programozó volt, aki *Captain Crunch* néven követte el máig legendás tetteit.

A 70-es évek végén a phreakerek tevékenysége főleg az ingyen telefonálgatásból, illetve az úgynevezett „Phreak-Joke"-okból, azaz vicces csínytevésekből állt. Például valakinek az otthoni telefonszámát egy nyilvános telefonéra cserélték, így akárhányszor felvette a telefont az illető, egy géphang közölte vele, hogy legyen szíves bedobni 25 centet. Máskor az ügyfélszolgálatos operátor helyett jelentkeztek be, és az előfizetőket az *„igen, a szám 8750 és fél – tudod hogy kell beütni a telefonon a felet, mamikám?"* és hasonló mókákkal idegesítették. Mivel nem volt pénze saját számítógépre, csak egy modemet hordott a zsebében: a helyi *Radio Shack* áruház bemutató gépeit használta első töréseihez. A vicceken kívül nem is csináltak mást, mígnem egyszer egy kicsit mellétrafáltak a tréfálkozással.

Az első betörés

Az első betörés, ami Kevin nevéhez fűződik, 1981-ben történt egy hétvégén: két barátjával Los Angeles belvárosában, a Pacific Bell's COSMOS épületében jártak, egész pontosan a telefonközpontban. A COSMOS a *Computer System for Mainframe Operations* rövidítése: ez a rendszer több nemzetközi telefontársaság (és előfizetőik) adatait őrizte és rendszerezte akkoriban. Kevin és a kis csapat eleinte semmit sem szándékoztak tenni azon felül, hogy „megnézik" a központot: a sors azonban úgy hozta, hogy az egyik biztonsági őr nem megfelelően végezte munkáját, így ők egy olyan szobába jutottak, ahová látogatóknak nem lett volna szabad. Ez még nem is lett volna baj, de az itt található COSMOS felhasználói kézikönyvet és egy jelszólistát (benne kilenc Pacific Bell's központi iroda belépési kódjával) viszont rögtön felmarkolták. Hogy a móka teljes legyen, az asztalon heverő egyik névjegyzékbe beírták beceneveiket (sőt még szegény „Captain Crunch" nevét is), mellé pedig hamis telefonszámokat adtak meg: ezek legtöbbje nyilvános telefonokra volt irányítva, azaz „routolva", megszokásból legtöbbször a közeli Van Nuys kávézó nyilvános készülékére. Ez a csíny azonban egyrészt már bőven illegálisnak minősült, másrészt a tökéletestől igen messze állt – le is buktak hamarosan. A Pacific menedzsere megtalálta a „vicces" neveket és számokat, majd rögtön feljelentést tett a rendőrségen, s a nyomozás elkezdődött. Kevin egyik társának volt barátnője (talán bosszúból) nyomra vezette a rendőröket: Mitnicket és két társát napokkal az eset után már le is tartóztatták. A vád „számítógépes adatok megsemmisítése és manipulálása", valamint az „operátor bizalmas adatainak az eltulajdonítása" volt: Az akkor 17 éves Kevin három hónapot töltött a Los Angeles-i *Juvenile Detention Center-ben*, valamint egy év próbaidőt is kapott. A kálvária elkezdődött...

Fehéringes bűnöző – bilincsben...

Nincs visszaút

Kevin szabadulása után öreg Nissanjára egy *X-HACKER* feliratú speciális rendszámtáblát igényelt, s ebből talán sejthető, hogy első letartóztatása nem inspirálta túlzottan a jó útra térésben. Ahelyett, hogy megpróbált volna elhelyezkedni és beilleszkedni, minden tudását és energiáját arra fordította, hogy amennyire lehetséges kiképezze magát a számítógépes és kommunikációs rendszerek biztonságával kapcsolatban – mindezt persze egyáltalán nem jó szándékúan. Ebből következett, hogy a 80-as években Mitnick szinte mindennap szembekerült a rendőrséggel, kisebb, nagyobb ügyek kapcsán.

Következő letartóztatására az *University of Southern California* egyetemi rendőrsége kerített sort, 1983-ban. Az egyetemen előzőleg már voltak problémái, amikor az ARPAnet (az internet elődje) szervereire tört be, ezúttal azonban az egyik egyetemi gépteremből (állítólag előadás alatt) az ARPAnet-en keresztül a Pentagon számítógépén turkált úgy, mintha csak a sajátja lenne. A Pentagon adataira – érthetően – nagyon háklis az amerikai igazságszolgáltatás: Kevin ezúttal már hat hónapot kapott, a vád „állami dokumentumok jogosulatlan használata" volt. Letartóztatásai úgy tűnik rossz hatással voltak rá, minden szabadulása után még nagyobb erővel hackerkedett, miközben igyekezett „tisztára mosni" magát. A tárgyalás után törölte a bíró bankszámláját, majd egy időre eltűnt. Később visszatért az Egyesült Államokba, ám alig, hogy újdonsült barátnőjével *Thousand Oaks-ba* költözött, 1987-ban illegális te-

„Amit be lehet csukni – azt ki is lehet nyitni…"

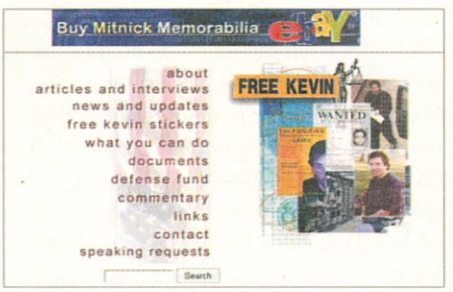
„Nem vagyok ártatlan, de nem én követtem el a nagy részét azoknak a bűnügyeknek, amelyekkel most vádolnak. Mondhatni, bűnbakot csináltak belőlem. Tanultam a hibáimból. Rengeteg tervem van a jövőre vonatkozólag, de a hackelés nincs ezek között" – Kevin Mitnick, a szabadulása után.

Kevin egyik fiatalkori példaképe *Richard Stallman,* egy úgynevezett *old school hacker.* Richard egyáltalán nem fél a nyilvánosságtól vagy a lebukástól, ezért internetes „beceneve" sincsen… Szaktudása kimagasló: miután elvégezte a Harvardot, 1971-ben az utcáról besétált a *MIT's Artificial Intelligence* laboratóriumába, és ott rögtön munkát kapott. Richard első „betörését" 16 évesen követte el 1969-ben: az *IBM New York Scientific Center* központi számítógépébe hatolt be, pusztán azért, mert kíváncsi volt arra, hogy mi lehet azon a gépen, amit ennyire védenek…

lefon-hitelkártyaszámok használata miatt kereste őt fel a rendőrség. A vádak között ebben az esetben már szoftverlopás is szerepelt: a *Santa Cruz Operation* nevű kaliforniai szoftvercég szerveréről „vett kölcsön" pár fejlesztést. 1987 decemberében 36 hónap börtönbüntetést kapott.

1988-ban Mitnick és az egyik közeli barátja, *Lenny DiCicco* elektronikus háborút folytatott a Palo Alto kutatási laboratórium ellen, személyes indíttatásból. Lenny egy kis kaliforniai cégnél dolgozott mint rendszergazda, innen indították támadásaikat a fiúk. Kevin először megszerezte a *Digital's VMS minicomputer operating system* névre hallgató rendszert (azaz annak egy másolatát) – ezen a rendszeren futottak a kutatási központ számítógépei. A Palo Alto központ gépei az *EasyNet* nevű halózaton voltak (akkoriban még nem volt a szó mai értelmében vett internet, csak ARPAnet, EasyNet és egyéb különálló egyetemi és kutatási hálózatok). Kevin és Lenny szinte minden éjszaka beindították a modemeket, és ahová csak tudtak, betörtek. Habár a támadásokat szinte rögtön észlelték a központban, sem a rendőrség, sem az FBI nem tudta megállapítani honnan jönnek, mivel Mitnick manipulálta a telefonközpontokat, így nem lehetett lokalizálni az eredeti modemes hívás helyét.

Kevin rutinosan két számítógépet használt a Palo Alto laboratórium töréseihez: az egyik végezte magát a műveletet, a másik pedig a bounce telefonközpontjait figyelte, és figyelmeztette őt, ha az FBI megpróbálta „backtrace"-elni, azaz visszakeresni a hívást. Egy alkalommal az FBI nagyon közel jutott, amikor azonban



Free Kevin – szabadítsuk ki Kevint!

azonosítani kellett a hívót, akkor egy Malibuban található nyaraló telefonszámát kapták.

A hosszú macska-egér játék után végül a nyomozás már olyan méreteket öltött, hogy Kevin társa (aki eleinte csak gyerekes csínynek fogta fel a dolgot) nem bírta a nyomást, és mindent bevallott a főnökének. Máris megérkezett az FBI, és Mitnicket újból elkapták. A vád több millió dolláros szoftverlopás és károkozás volt, valamint az elkövető lenyomozására költött több mint kétszázezer dollárt is bevették a vádiratba: Kevin egy év börtönbüntetést és fél év „rehabilitációs" kezelést kapott. 1989-ben Las Vegasba költözött, és munkát vállalt mint programozó. Magával vitte azonban *Susan Thundert,* aki a 80-as évek elején alakult phreaker-csapatának egyik tagja volt. Ez idő tájt a nevét már felkapta a sajtó. Mivel akkoriban még egyáltalán nem voltak hackerek (illetve nem kaptak el egyet sem…), Kevin lett a média és az átlagamerikai szemében „a hacker".

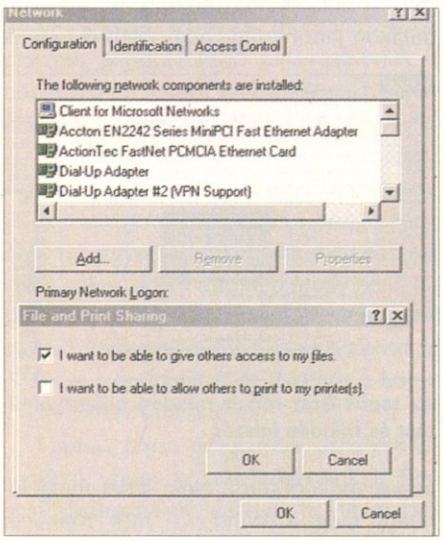
A szenzációéhes újságírók rengeteg körítéssel tálalták a palo alto-i betöréseket és az FBI kezdeti eredménytelenségét. Mitnickről olyan történetek keringtek, hogy egy számítógéppel és egy modemmel képes betörni a Pentagonba és elindítani az atomháborút. Természetesen az újságokban tálalt sztoriknak és találgatásoknak a fele sem volt igaz. Susannal való rövid együttélése és kisebb „balhék" után Mitnick a *San Fernando* völgybe költözött, és a *Tel Tec Detective Agency* névre hallgató irodában vállalt állást. Röviddel ezután érdekes módon a Tel Tec egyik számítógépéről valaki betört egy telefonszolgáltató üzleti adatbázis rendszerébe – Kevin ismét az FBI célpontjává vált. Mivel megszegte a „rehabilitációs" program szabályait (betört egy rendszerbe és felvette a kapcsolatot a vele együtt 1981-ben letartóztatott phreaker-banda egyik tagjával) ismét a törvény elé került. Ekkortájt terjedtek el azok a vélemények, amelyek szerint Mitnick „mindenre képes" – a börtönbüntetés mellett ezúttal még a mobiltelefon használatától is eltiltották. Nagyjából ebben a stílusban folytatta tevékenységét, egészen utolsó letartóztatásáig: 1995-ben öt évet kapott a *Sun Microsystem* és a *Motorola* hálózatának és szervereinek feltörése és az adatok illegális birtoklása miatt. Az ítélet magában foglalta, hogy az öt év letelte után további három évig nem használhat internetre kapcsolt számítógépet. Utolsó letartóztatása után indult a *Free Kevin* internetes akció, ami főleg a hackerek tiltakozását fejezte ki: rengeteg defeace született „Free Kevin" felirattal, nem is beszélve a matricákról, rendszámokról, újságcikkekről és weboldalakról. Kevin utolsó (és leghosszabb) büntetése alatt könyvet írt *The Art of Deception* (A megtévesztés művészete) címmel. ■

Kevin Free, azaz Kevin szabad, de vajon meddig?

Váratlan veszélyek

Az internetről számtalan veszély leselkedik a gyanútlan felhasználóra: hackerek, akik hozzáférhetnek a gépünkhöz, vírusok, amelyek tönkretehetik adatainkat, különböző kémprogramok, amelyek minden mozgásunkat nyomon követik. Cikkünkben összefoglaljuk a veszélyeket, és a védelezés módjáról is ejtünk néhány szót.

Ma már szinte nem is adnak el úgy számítógépet, hogy ne tennék lehetővé rajta a világháló elérését. Ez egyfelől remek dolog, másfelől viszont tisztában kell lennünk azzal hogy az internet egy olyan hálózat, ahol sok mindent elérhetünk, tehát ennek a fordítottja is igaz, minket is sokan megtalálhatnak. A hívatlan látogatók felfedik böngészőnk és Windowsunk verziószámát, elérhetik adatainkat. Ez természetes, ha a *mappáinkat mások számára is megnyithatóvá tesszük,*



A Control Panel/Network oldalán tilthatjuk le a fájlmegosztást

vagyis nem használunk jelszót, amikor megosztott fájlokkal és nyomtatókkal dolgozunk. Ha az alkalmazásainkat nem tesszük mások számára is elérhetővé, csökkenthetjük a behatolások számát. Ha a gépünk nem egy helyi hálózat része, akkor a *Control Panel/Network* menüpontnál ne engedjük meg a fájlok és nyomtató megosztását.

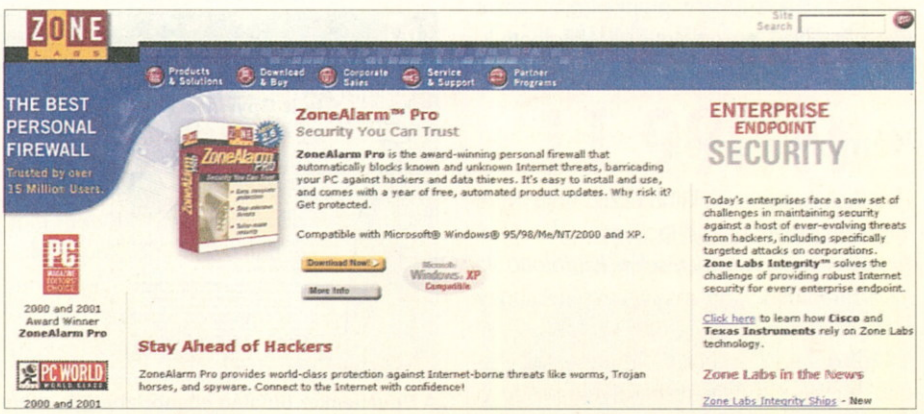
Vírusok

A vírusok hozzákapcsolják magukat más alkalmazásokhoz, azaz megfertőzik azokat. Az első példányok csak *a végrehajtható programok kódjaiban fordultak elő, de a scriptnyelvek megjelenésével már elektronikus levelekben, szövegdokumentumokban, Excel táblázatokban és egyéb alkalmazásokban is jelen vannak.* Némelyikük csak sokszorozza önmagát, mások törlik vagy felülírják adatainkat. Sajnos nincs olyan módszer, amellyel teljesen megszabadulhatunk tőlük. A jó vírusellenes programok, persze amelyek még nem jártak le, kezdeti lépésnek megfelelőek. Vannak ingyenes programok és olyan oldalak is, ahol online ellenőrizhetjük adatainkat, persze ezek meglehetősen lassúak.

Mindent ellenőrizni kell, ami gépünkre érkezik: *levelezéseinket, azok csatolt állományait, internetes letöltéseinket, a kölcsön kapott CD-ket.* Legyünk naprakészek, vagyis tudjuk, milyen újabb támadások ellen kell védekeznünk.

Trójai programok

Az olyan programokat soroljuk ebbe a csoportba, amelyeknek valamilyen titkos általában rossz hatása van,. Ha a gépünkre került, *a program azonnal kapcsolatot keres készítőjével,* amikor online vagyunk. Ilyenkor a gépünk szerverként működik, így megengedi a trójai program alkotójának, hogy a gépünkön azt tegyen, amit akar. Hozzáférhet bármelyik fájlhoz, programokat futtathat és a jelszavunkat is megszerezheti. A leghíresebb trójai programok listáját megtalálhatjuk a **www.sub-7files.com** címen. A személyes tűzfalak, mint például a *ZoneAlarm* (**www.-zonelabs.com**) megakadályozhatják, hogy a trójai programmal érintkezzen a tulajdonosa, de erre nincs mindig garancia, mert egyik tűzfal sem tökéletes. Az egyetlen igazi védekezés, ha nem indítunk el gyanús alkalmazásokat a gépünkön. Ezért figyeljünk arra, milyen programok futnak, minden gyanús lehet, amit elektronikus levélben kapunk, még akkor is, ha az a barátunktól érkezik. A bináris csatolt állományok a hírcsoportokban veszélyt jelentenek. *Csak olyan ingyenes programokat töltsünk fel a gépünkre, amelyek megbízható forrásból származnak.* Minden letöltött fájlt ellenőrizni kell a legfrissebb vírusirtó programmal, de nem árt egy igazi trójai felismerő program sem (**www.moosoft.com**). Ilyen ingyene-



A ZoneAlarm segít kiszűrni a trójai programokat

A DiamondCs az egyik legjobb trójai program-felismerő alkalmazás

sen letölthető például a **www.diamondcs.com.au** címről.

Sütik (cookies)

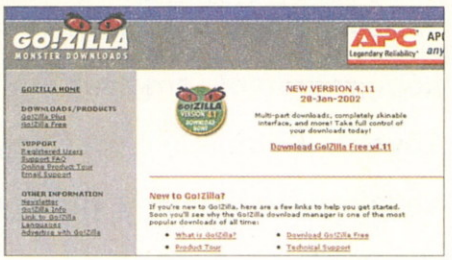
Tegyük fel, hogy vásárolni akartunk egy internetes üzletben, de valami miatt megszakítottuk a kapcsolatot. Mikor újból felkeressük ezt az online üzletet, bevásárló kosarunkban megtaláljuk az előző alkalommal kiválasztott termékeket. Ez amiatt lehetséges, mert az üzlet „sütiket" (idegen szóval: cookies) küldött a gépünkre, amelyek a rendelésünkről tartalmaztak adatokat. Más oldalak nem tudják értelmezni ezeket, csak ahonnan küldték őket.

Sok ilyen „hasznos" vagy éppen váratlan meglepetés érhet bennünket. A hirdetési csíkok (bannerek) segítséget nyújthatnak a vállalatoknak ahhoz, hogy sütiket helyezzenek el a rendszerünkben, amelyek egyedi azonosítók is lehetnek. Így tudják nyomon követni, milyen hirdetéseket láttunk már. Amikor olyan oldalakra látogatunk, ahol ugyanaz a cég hirdet, amelyik előzőleg sütit helyezett el a gépünkön, egy új hirdetéssel fog jelentkezni. Ezek nem veszélyesek, mert nem törődnek azzal, kik vagyunk, csak arról tudnak, hogy olyan oldalakon járunk, ahol ők hirdetnek.

A **www.netscape.com** oldalon ellenőrizhetjük, milyen sütiket kaptunk eddig. Ezeket kitörölhetjük egyenként, blokkolhatjuk, vagy engedélyezhetjük is a működésüket.

Kémprogramok

A kémprogramok kifürkészik, hogy mire vagyunk kíváncsiak. *Megjegyzik és rögzítik, hogy milyen hirdetésekre kattintottunk.* Ez a hirdetőknek ad majd segítséget, hogy milyen reklámok a legsikeresebbek. A későbbiekben ilyen jellegű hirdetésekkel fognak bennünket felkeresni. Ilyen program például a *Go!Zilla*. A telepítés során a program közli is, hogy a háttérben dolgozik, információkat gyűjt és továbbít, amelyek a hirdetésekre vonatkoznak. Amikor elindítjuk a programot, a hirdetési részben megtaláljuk a kémprogram saját kezdő menüpontját is. Itt részletesen olvashatunk arról, mi a feladata ennek a programnak, de ki is törölhetjük azt. Bár lehet, hogy ennek ellenére adatokat küld továbbra is gépünkről.



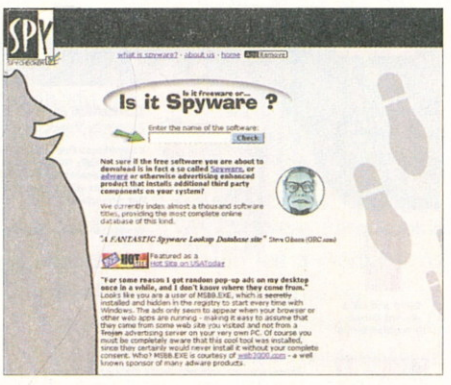
A Go!Zilla figyeli, milyen az érdeklődési körünk

A LavaSoft segít eltávolítani a kémprogramokat

Ha ez zavarna valakit, annak az igazi megoldást az nyújtja, ha nem használ adware (ingyenes, de cserébe hirdetéseket kell néznünk) programot, hanem csak regisztrált változatot.

Jó tanács: olvassuk mindig el a licencszerződést, és csak utána kattintsunk az OK gombra. Vannak olyan programok, amelyek segítenek eltávolítani a kémprogramokat **(www.lavasoft.com)**.

A **www.spychecker.com** címen találhatunk egy listát azokról a programokról, amelyek „kémkedni" tudnak.



A Spychecker oldalán ellenőrizhetjük, mely programok kémkednek

Fertőzött alkalmazások

A hálóról letöltött programok *férgeket* tartalmazhatnak. HTML kiterjesztésű leveleinkhez olyan programok tartozhatnak, amelyek az engedélyünk nélkül indulnak el a gépünkön.

Az üzenettovábbító programok is veszélyesek lehetnek. Ezeknek mindig a legfrissebb változatát használjuk, és kísérjük figyelemmel a legújabb biztonsági híreket.

Leskelődő programok

Könnyen ellenőrizhető, hogy milyen programok futottak a gépen. Ez akkor lehet veszélyes, ha nem a saját gépünkön dolgozunk. Az *Iopus Starr* mindent rögzít: milyen billentyűket ütöttünk le, mely oldalakon jártunk úgy, hogy nem is tudunk

Az Iopus Star rögzít minden billentyűleütést és minden jelszót

annak működéséről. Nem lehet megjeleníteni még a Windows Task Manager programjával sem. Ha felfedezzük jelenlétét, nem tudjuk kitörölni az *Uninstall* lehetőséggel, mert jelszóval védett.

Vannak módszerek, amelyekkel legyőzhetőek az ilyen jellegű programok. Például indítsuk újra a rendszert, közben a **Ctrl** gombot tartsuk nyomva. A megjelenő menüből válasszuk a *Safe Mode-ot*. Ebben az üzemmódban, már nem fog elindulni az Iopus Starr. Keressük meg a program végrehajtható fájljait a lemezen, és közülük néhányat nevezzünk át vagy töröljünk.

Támadó alkalmazások

Vannak olyan programok, amelyek megjegyzik, hogy merre jártunk böngészéseink során, majd keresgéléseink tárgyának megfelelő hirdetéseket juttatnak el képernyőnkre. Ilyen program például a *GoHip* **(www.gohip.com)**, amelyik állandóan hirdetéseket jelenít meg gépünkön és újabb oldalakat fűz *„Kedvenceink"* lis-

A Gohip állandóan hirdetéseket jelenít meg gépünkön

tájához. A **www.gohip.com/remove_browser_enhancement.html** címen arra kaphatunk tanácsot, miként lehet ezt elkerülni. Sokszor a rossz programozás is okozhat gondot. Több alkalmazásnak a böngészőhöz közel kell dolgoznia, ezért azok proxyként installálják magukat, vagyis ellenőrzik az internetkapcsolatunkat. Amikor azok nem dolgoznak, vagy eltávolítjuk a programokat, akkor a böngészőnk nem fog egyetlen oldalt sem megjeleníteni. Ilyenkor ki kell törölni a proxy beállításokat, ez az egyetlen megoldás. Válasszuk a *Tools/Internet Options/Connections/Lan Settings* menüpontot, *és töröljük a Use a proxy server sort.*

Vannak olyan programok, amelyek ellenőrzik, hogy a számítógépünkön futó más alkalmazások legálisak-e. Ha lejártak már, akkor megszakítják azok működését, bontják az internetkapcsolatunkat, törlik a képernyőnket. Ehhez azonban szükségük van az IP-címünkre. Ez azonban könnyen megszerezhető, ha beszélgetőcsatornát vagy állandó üzenetküldő rendszert használunk, mint például az *ICQ-t.* Vigasztaló tény lehet, hogy ezek a támadások nem okoznak sérülést adatainkban, csak megszakítják a program működését. Ezután minden visszaállítható az eredeti állapotába. Rossz hír, hogy nehéz ellenük védekezni. Legjobb megoldás persze, ha legális Windows programot használunk.

Helyi hálózati veszélyek

Figyeljünk arra, hogy mások ne tudjanak arról, milyen oldalakat látogattunk meg az interneten. Ehhez tüntessük el a nyomokat magunk után az Internet Explorerben. Kattintsunk a *Tools/Internet Options/General* menüpontnál a *Delete*

Bizalmas adatainkat érdemes valamilyen programmal titkosítani

History és Cookies pontra, majd válaszszuk a fájltörlés lehetőséget. Ellenőrizzük az offline tartalmat, majd kattintsunk az OK gombra. Ezután kattintsunk a *Content* gombra. Töröljünk ki mindent, ami az *AutoComplete* címszó alatt található, majd minden személyes adatot a *My Profile* címszónál.

Arra is kell figyelni, kik vannak a közelünkben, vagyis kik kerülhetnek fizikai kapcsolatba a gépünkkel. Ők ugyanis könnyen kideríthetik, mit kerestünk a hálón, mi a jelszavunk, bankszámla számunk, olyan programot tölthetnek fel a gépünkre, amely minden gombnyomásunkat rögzíti. Ilyenkor persze ne a családtagokra gondoljunk.

Érdemes olyan eszközöket, például az *Encrypted Magic Folders* vagy a *PGP programját* használni, amelyekkel bizonyos mappákat titkossá tehetünk **(www.pc-magic.com, www.pgp.com).** Ne felejtsük el, hogy a Windows programmal nem lehet kitörölni úgy a fájlokat, hogy azok tartalmát később ne lehetne visszaállítani. Olyan programot használjunk a törléshez, amelynek nincs meg ez a lehetősége, de ellenőrizzük, hogy valóban nem lesz-e már szükségünk a törlendő adatokra. *Tegyük jelszóval védetté gépünket az alkalmi látogatókkal szemben.* ■

Feszítővas helyett

Egy súlyos lefagyás esetén mentőprogramok életszthetik újra a Windowst, ám ezek – amint az cikkünkből is kiderül - betörők segédeszközeként is szolgálhatnak.

A biztonságra törekvő Windows felhasználók komplikált bejelentkezési jelszavakat találnak ki, sosem rendszergazdaként jelentkeznek be alaphelyzetben, és vírusfigyelőkkel, valamint tűzfalakkal védik magukat. Ám aki fizikailag hozzáfér a PC-hez, az mindezt megtörheti, minden tiltást kikerülhet és alkalmas betörőszoftverrel hozzáférhet a rendszerhez. Ez persze kapóra jön, ha elfelejtettük volna a rendszergazda jelszót, de kellemetlen, ha illetéktelenek férnek a számítógépünkhöz.

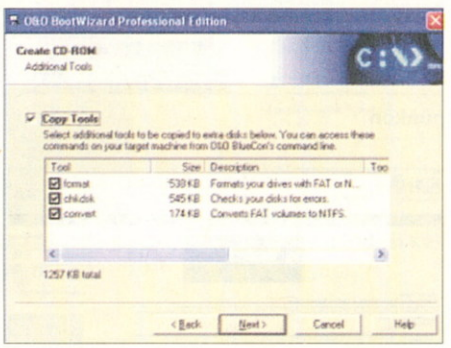
Az itt bemutatásra kerülő hackerprogramokat persze csak a saját magunk számára és csakis végszükség esetén szabad használni. Aki idegen PC-t akar manipulálni, az büntetőjogi következményekkel számolhat.

Mellesleg megtörjük

Aki olyan PC-n dolgozik, amelyet többen is használnak, az ki van téve annak a veszélynek, hogy a jogos felhasználók a saját jelszavukkal bejelentkezve egyszerű próbálkozással felkutatják más felhasználók jelszavát. Mivel a lehetséges bejelentkezési jelszavak kézi próbálgatása nehézkes és sokáig is tartana, rosszindulatú kortársaink *jelszótörő programokat* használnak. Ilyen a *PwlTools 6.80* a Windows 9x/ME alatt, vagy az *ntPassword 4.0* a Windows NT/2000/XP alatt. Mindkét program szisztematikusan végigteszteli az összes elképzelhető karakterkombinációt. A rövid jelszavakat gyorsan meg lehet fejteni. A másik támadási pont a Windows 9x/ME azon tulajdonsága, hogy átmenetileg egy jelszó cache-ben tárolja a megadott jelszavakat. A PwlTools pillanatok alatt megjeleníti a pufferelt jelszavakat.

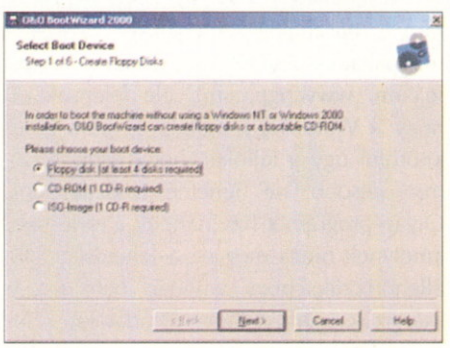
Rendszergazda jelszó

Ha a jelszó elfelejtése miatt semmilyen rendszergazdai hozzáférés sincs a PC-hez, akkor a jelszó-visszaállítás néhány másodperc alatt elvégezhető az *O&O BlueCon 4*-gyel. A szoftver meg sem próbálja megtalálni az eddigi jelszót, hanem egyszerűen felülírja. A BlueCon-nak mindegy, hogy a Windows FAT, FAT32 vagy NTFS partícióba lett-e telepítve, vagy hogy egy Windows XP munkaállomásról, esetleg egy Windows 2000 Advanced Serverről van-e szó, a jelszót mindegyiknél visszaállítja.



A Bluecon 4 a jelszó-visszaállításában segít

A szoftver telepítését követően indítsuk el az *O&O BootWizard Prót*, amely összegyűjti a támadáshoz szükséges fájlokat, és ezekből egy indító flopilemezt vagy egy ISO *CD-image*-et készít. Ehhez a varázsló lekér néhány állományt a Windows telepítő CD-jéről. Opcionálisan, a Windows jelszónktól függetlenül, a bootadathordozóink védelmére is készíthetünk jelszót.

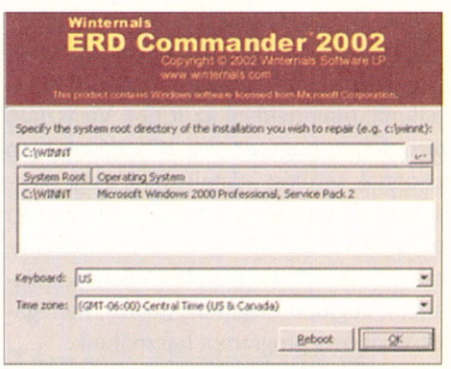


A BootWizard Pro összegyűjti a támadáshoz szükséges fájlokat

A rendszergazdai jelszó feltöréséhez a bootlemezről kell indítanunk a PC-t. Ha a boot-varázslóban kiadtunk egy jelszót, akkor azt most meg kell adnunk. Ellenkező esetben a BlueCon közvetlenül konzol üzemmódban indul el, ami a DOS parancssorra emlékeztet. Egy meglévő jelszó megváltoztatásához a *passwd administrator [Neues Kennwort]* (új jelszó) parancsot kell kiadni. Az *administrator* helyett bármelyik másik létező fiókot is megadhatjuk. Az üresen hagyott jelszó törli a meglévő jelszót, így a felhasználónév mellé nem kell megadni jelszót a bejelentkezéshez. Kb. 30 másodpercnyi várakozási időt követően a BlueCon végrehajtja a szükséges változtatásokat a Windowsban. A *reboot* paranccsal a BlueCon-ból kilépünk, és a Windows újraindul.

Az O&O BlueCon használatánál egyébként lényegtelen, hogy a támogatott Windows verziók melyikével készült a boot-CD.

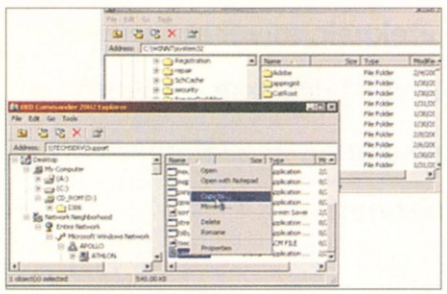
Betörés a Windowsba



Az ERD Commander 2002 is alkalmas a betörésre

Ha a behatoló már hozzáfér a PC-hez, akkor a helyi merevlemezen található összes adatot elérheti. Nehéztüzérséget vonultat fel az *ERD Commander 2002* is. Ez a betörőprogram szintén egy indításra alkalmas CD-n vagy flopin alapszik, ame-

lyet a felhasználó egy varázsló segítségével lépésről lépésre hozhat létre. A BlueCon-nal ellentétben, az ERD Commander egy, a Windowséra emlékeztető grafikus felületet indít el, amely felkínálja az összes meghajtó elérését, és megengedi a rendszergazdai jelszó törlését. Különösen trükkös a helyi TCP/IP-hálózat elérése, hogy a Windows jogosultsági rendszer kikerülésével fájlokat lehessen egy másik számítógépre továbbítani. Két to-



Az ERD Commander egy, a Windowsra emlékeztető grafikus felületet indít el

vábbi betörőprogram is napvilágot látott már ugyanettől a gyártótól: az *NTFSDOS Professional 4.0* és a *Remote Recover 2.* Míg az NTFSDOS egy bootlemezzel csupán az összes NTFS partíció írását és olvasását teszi lehetővé, addig a startlemezzel történő indítás után a helyi PC összes adatának teljes TCP/IP-n keresztüli távelérését is felajánlja.

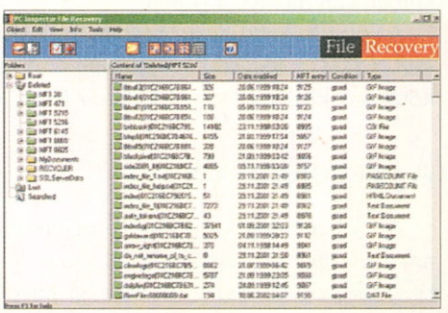
A törölt fájlok gyors visszaállítása

A megfelelő hackereszközökkel azok a törölt fájlok is előbányászhatók, amelyekről a jogos tulajdonos azt hiszi, hogy már régen megszabadult tőlük. Ez különösen akkor alattomos, amikor biztonsági okokból érzékeny adatokat semmisítünk meg a Windows alatt, például személyzeti aktákat, bizonyítványokat, egyenlegeket vagy a saját adóbevallásunkat. Ha a használt merevlemezünket vagy PC-nket továbbadjuk másnak, a lemezek formázása csalóka biztonságot nyújt csupán.

Ezekben az esetekben speciális programokat lehet használni, amelyeket eredetileg az adatok megmentésére szántak. Különösen sokoldalú az adatok visszaállításában az *EasyRecovery DataRecovery 6.0*, amelyet egy mentőlemezről (flopi) lehet indítani.

A program végigfésüli a már nem indítható partíciókat (FAT 16, FAT 32, NTFS), és megkeresi a törölt, de még felül nem írt fájlokat. Az EasyRecovery ilyenkor nem egy törölt File Allocation Table esetleges adataira vagy ennek másolatára hagyatkozik, hanem fájldarabok után kutatva teljes cluster-keresést hajt végre a teljes adathordozón. A keresést fájlszűrőkkel lehet behatárolni, például hogy csak az Office dokumentumok legyenek figyelembe véve. Az EasyRecovery egy rendezhető fastruktúrában jeleníti meg a megtalált fájlokat. Ekkor az esetek többségében elvesznek az eredeti fájlnevek, helyettük folyamatos számozást használ.

A szoftver ezt követően a kívánt könyvtárba másolja be a visszaállított fájlokat. A bootflopis megoldás terjedelmes restaurálások esetében hamar elakad a saját korlátain, ezért célszerűbb abba a PC-be beépíteni az érintett merevlemezt második merevlemezként, amelyiken a Windows alatt az EasyRecovery fut. Az 550 euróba kerülő professzionális változat egyébként további javító funkciókat is kínál sérült Office-dokumentumokhoz és ZIP-fájlokhoz.



Egy remek ingyenes fájlvisszaállító program: a PC Inspector File Recovery

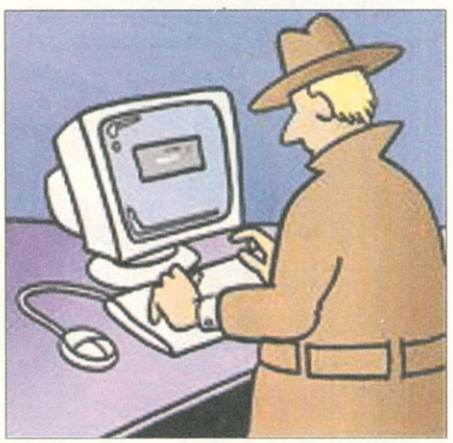
A freeware *PC Inspector File Recovery 3.0* a *Convar* cég terméke. Ezt a programot szintén egy második független lemezegységre kell telepíteni, és ott kell futtatni is.

A program analóg módon működik az EasyRecovery-vel és egy állapotoszlopban jeleníti meg a javítási esélyeket. A *jó* esetén sok esélyünk van, de még a *rossz* esetén is érdemes megpróbálkozni a visszaállítással. Ehhez a művelethez kattintsunk az egér jobb oldali gombjával a fájlra, és adjuk meg, hogy melyik mappába akarjuk tárolni. A PC Inspector a FAT16/32 és NTFS fájlrendszereket is támogatja. A program jelentős részben azonos Alexander Grau *Drive Rescue 1.9c* freeware segédprogramjával, amelynek a forráskódja ingyenes. ■

Ne mondd meg ... kitalálom!

Az egyik legnagyobb akadályt változatlanul az okos jelszavas védelem jelenti a hackereknek, mivel az interneten és a helyi számítógépeken is gyakran jelszavak védik a fájlokat és a postafiókokat a jogosulatlan hozzáférések ellen. Azonban mint tudjuk: minden feltörhető...

A jelszavak kiderítésére, illetve feltörésére különböző lehetőségek vannak. Az egyik legfontosabb a *Social Engineering*, amellyel a fontos adatok jelszótulajdonosoktól való megszerzését jelölik. A kreativitás, amellyel ilyenkor eljárnak, hihetetlen. Tehát ne hagyjuk, hogy ismeretlenek olyan információkat csaljanak ki tőlünk, amelyeket senkinek sem adnánk meg önként. A Social Engineering történhet mondjuk egy telefonhívással, amelyben a főnökünk keresztnevét kérdezik – kulcsszó: e-mail-cím.



Jelszótörés

A legtöbb felhasználó nem túl ötletes egy értelmes jelszó kitalálásánál. Ezért a rosszul választott jelszavak kihasználása a hackerek egyik legjobban elterjedt támadófegyvere.

A jelszavak megadásánál a következő alapszabályokat kell(ene) betartani:

- ne legyen öt karakternél rövidebb
- semmi duplázás, tehát ne legyen „hhaalloo",
- ne legyen szabványos,
- semmi születési dátum és hasonlók,
- ne legyenek olyan szavak, amelyek benne lehetnek a jelszólistákban vagy a szótárakban.

A jó jelszavak több mint tíz karakterből, alfanumerikus karaktersorból (például km134Hs9), vegyesen kis- és nagybetűkből állnak.

Teljesen értelmetlen a jelszóhasználat, ha mindenütt ugyanazzal a jelszóval dolgozunk, esetleg egy cetlit teszünk a billentyűzet alá vagy a monitorra, és ráírjuk a jelszavunkat, netalán a jelszó egy fájlban van mentve a gépen.

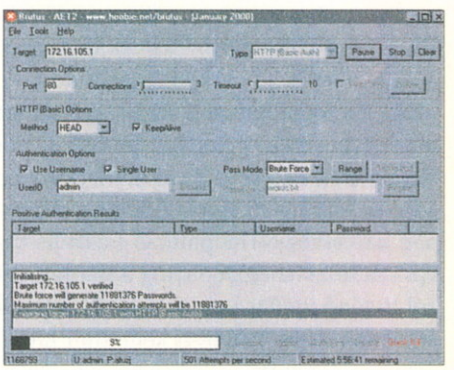
A jelszót *kettő-négy hetente cserélni kell.* Ezzel a fogással meghiúsíthatjuk a korábban kikémlelt jelszó felhasználását.

A jelszófeltörők

A *jelszófeltörők* olyan programok, amelyek jelszavakat fednek fel, hogy kikerüljék az alkalmazott biztonsági intézkedéseket. A jelszót a legritkább esetben fejtik vissza, ehelyett egy névről nagyon jól ismert eljárást, a *Brute Force*-ot használják. A Brute Force annyit jelent: nyers erő. E programok nem tesznek mást, mint nagyon nagy sebességgel próbálják ki az egyik lehetséges jelszót a másik után, amíg megtalálják az igazit.

Egy példa az ilyen programokra a *Brutus.* A Brutus jelszófeltörő az internet-accountok valamennyi variánsához (FTP, HTTP, POP3, Telnet, NetBios stb.). Az internetes jelszavak valamennyi fajtájához szívesen használják.

A *Target* mezőbe be kell írni a kikémlelendő fél URL-jét vagy IP-címét. Ezután ki lehet választani a támadás fajtáját, és szükség szerint szólistákat is be lehet tölteni, amelyek, ha a jelszó a listán van, igencsak megrövidítik a feltörést. Egy további, a támadásokhoz hasznos tulajdonság egy beépített proxy, amely megakadályozza, hogy vissza lehessen követni a támadót.



Amikor a „nyers erő" dolgozik

Hogyan válasszunk jelszót?

A válasz nagyon egyszerű: sehogy. Ha ugyanis elkezdünk gondolkodni azon, hogy mi legyen a jelszavunk, máris elin-

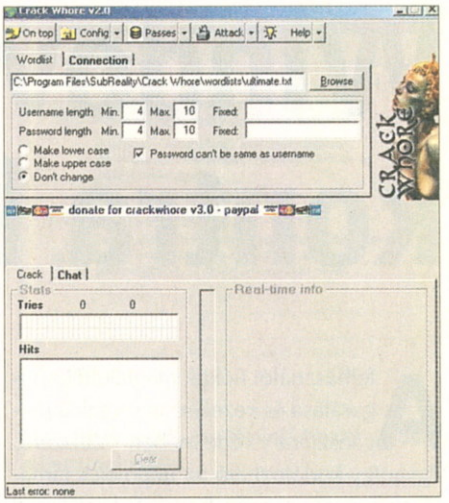
Ismert felhasználói nevek jelszavainak a kitalálása

A jelszótörő ennél az eljárásnál csak egy user névvel próbálkozik, amelyet előre meg lehet adni, mert az már ismert, de nincs meg a hozzá tartozó jelszó. Így lenne ez például akkor is, ha elfelejtettük a fiók-jelszavunkat.

dítottunk egy folyamatot, s a végén óhatatlanul valami személyes, hozzánk kötődő kódsort találunk ki. A legrosszabb esetek a szokásos születésnap, névnap, a feleségünk vagy a kiskutyánk beceneve és egyéb dátumok, autónk rendszáma és mindezek keveredése. Ezeket ugyanis nagyon könnyen kitalálja bárki, aki csak egy kicsit is ismer minket. Az sem megoldás, ha személyes számainkat/neveinket választjuk jelszóként, de összekeverve vagy anagramma gyanánt sem jelentenek jó megoldást. Egy jó kódtörőnek ugyanis teljesen mindegy, hogy a jelszó helyesen *„csöpi"* mert így hívják a kutyusunkat, vagy összekevertük a betűket és a jelszó „öpsci" lett. Szintén nem sokat javít a helyzeten, ha a jelszó mögé teszünk egy-két számot, pl. *csöpi11* vagy *öpics412*. Az igazán profi hacker ugyanis, miután mindent megtudott rólunk (néhány elvetemült hacker képes a kiszemelt áldozat házi szemeteskukájában is turkálni blokkok, levelek, csekkek és egyéb személyes infók után kutatva…) a fejlettebb kódtörő szoftverekbe egyszerűen beírja a személyes adatainkat (születési dátumunkat és hasonlók) és minden hozzánk kapcsolódó kifejezést, köztük a *csöpi* szót is. A szoftvernek pedig teljesen mindegy, hogy *csöpi* vagy *icsöp987*. A tanácsunk a jelszóválasztáshoz tehát a következő: ha azt akarjuk, hogy nehéz legyen feltörni a jelszavainkat, akkor válasszunk valami teljesen eszement, „véletlenszerű" kódsort, variálva a kis- és nagybetűket és számokat. Az ideális jelszó tehát valahogy így néz ki: *94Za8qerT*. Az ilyen jelszó csak az úgynevezett *Brute Force* (*„nyers* erő") eljárással törhető fel, aminek a lényege hogy a kódtörő program minden variációt kipróbál – de ez nagyon időigényes, és a jelszavak tekintetében nem az a cél, hogy ne lehessen feltörni, hanem az, hogy sokáig tartson! ■

A titkos kérdések

Az interneten a különböző oldalak biztonságra ügyelő szolgáltatói *jelszókérdések* vagy *titkos kérdések* megadását kínálják, hogy a felhasználónak lehetővé tegyék, megváltoztatni a jelszavát, ha elfelejtette. Gyakran lehet ilyen kérdésekkel találkozni: „Mi a hideg ellentéte?" Ez természetesen rossz választás, mert így minden támadónak lehetővé tesszük a jelszavunk tetszés szerinti megváltozatását.



Jelszófeltörés folyamatban – persze teljesen automatikusan

Windows XP kontra hackerek

A Windows XP Home Edition az első olyan Microsoft operációs rendszer, amely magáncélú, vagyis otthoni felhasználáshoz is határozottan elkülöníti egymástól a felhasználói fiókokat, és ezzel lehetővé teszi a magánjellegű adatok védelmét. Ehhez azonban megfelelően kell konfigurálni, és néhány biztonsági beállításra is szükség van.

A felhasználói fiókok megfelelő konfigurálása és kezelése nemcsak a magánszféra védelmében célszerű. Ugyanígy korlátozható az internetes támadások hatása is, még ha *csak korlátozott jogokkal* jelentkeztünk is be a Windowsba.

Több felhasználói fiók kialakítása

Az operációs rendszer már a telepítésnél megengedi, hogy *több felhasználót* adjunk meg. Ekkor célszerű a felhasználók számánál eggyel több fiókot létrehozni, tehát ha ketten használják a PC-t, akkor három hozzáférés legyen. Így saját magunknak két fiókunk van, egy a hétköznapi használatra való korlátozott és egy olyan, amelynek rendszergazdai jogai vannak. Ez utóbbit csak a számítógép konfigurálásához használjuk.

Nem árt, ha több felhasználói fiókot is nyitunk a rendszerünkben

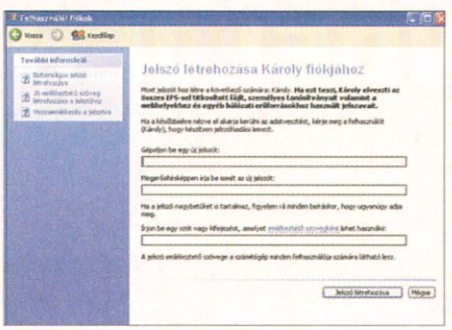
Telepítsük újra a Home Edition-t, és készítsünk például három fiókot. Az *Admin* legyen a rendszergazda, továbbá legyen egy *Károly* és egy *Brigitta* nevű fiók is. A PC indításánál ez a három fiók fog választékként megjelenni. Ezután először az *Admin* fiókba jelentkezzünk be, mert a hétköznapi felhasználók csak a saját fiókjuk beállításain változtathatnak, de nem készíthetnek újat vagy nem változtathatnak meg egy idegen fiókot.

Ha már használjuk a Windows XP-t, akkor készítsünk még két további fiókot.

Az új fiók létrehozásának első lépése

Ehhez kattintsunk a *Start* gombra, a *Vezérlőpultra*, a *Felhasználói fiókokra*, majd az *Új fiók létrehozására*. A következő lépésben adjunk a fióknak egy nevet (pl. Károly), és készítsük el a fiókot a *Továbbbal* és a *Fiók létrehozásával*. Ismételjük meg ezeket a lépéseket a második fiók létrehozásakor is.

Most valamennyi fiókot védjük le jelszóval. Ehhez a felhasználói fiókok ablakban válasszuk a *Fiók megváltoztatását*, majd kettős kattintással válasszunk ki egy fiókot.



Jelszóval védhetjük az új fiókot

A következő ablakban kattintsunk a *Jelszó létrehozása* kapcsolóra, és mindkét mezőbe adjuk meg a titkos jelszavunkat. Ez a jelszó biztonsági okokból legalább nyolckarakteres legyen. Vegyük figyelembe, hogy a Windows a nagy- és kisbetűk között is különbséget tesz. Jegyezzük meg a jelszavunkat! A *Jelszó létrehozása* kapcsolóra kattintással a fiók a jövőben jelszóval védetté válik.

Ismételjük meg ezeket a lépéseket a többi fióknál is, s a többi személy is írja fel a saját jelszavát. Ennek hatására az összes fiók megnevezése alatt a *Jelszóval védve* szöveg jelenik meg.

Most pedig – a rendszergazda fiókjának kivételével, amelyen keresztül bejelentkeztünk – korlátozzuk be a másik két fiók jogosultságát. A kívánt fiókra kettőt kattintva egy új ablak nyílik meg, ahol a *Fióktípus módosítását* választjuk. A következő lépésben a *Korlátozott* bejegyzést kell aktiválnunk, és a *Fióktípus módosításával* kell kilépnünk. Ezt az eljárást végezzük el a második korlátozandó fiókkal is.

Jó tudni, hogy az új fiókok még akkor sem korlátozódnak automatikusan, ha felhasználtuk az XP-hez való *Service Pack 1*-et.

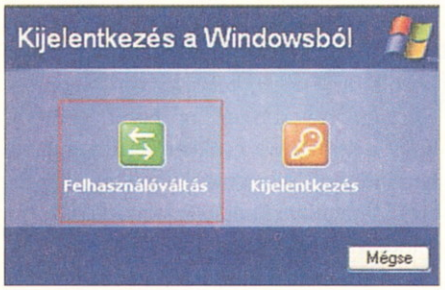
A több XP-hozzáférés előnye

Lehet, hogy felmerül a kérdés, mire jó ez a sok cécó? Pontosan mi is választja el a különböző fiókokat?

Mindenekelőtt praktikus a *gyors felhasználó átkapcsolás*. Így a család valamelyik tagja gyorsan el tud intézni valamit a fiókjában anélkül, hogy abba kellene hagynunk a munkánkat.

Kattintsunk a *Start* kapcsolóra, majd a *Kijelentkezésre*. A Windows kijelentkező képernyője jelenik meg, amit a Microsoft egyébként gyors felhasználóváltásnak is hív.

A *Felhasználóváltáson* keresztül a Windows ismert kijelentkező képernyője



A Microsoft gondoskodott a gyors felhasználóváltásról

jelenik meg, ahol bejelentkezhetünk egy másik fiókba. Az eredeti fiókba is ugyanígy jutunk vissza, vagyis ott folytathatjuk a munkát, ahol az imént abbahagytuk.

Ez az átkapcsolás megbízhatóan működik, de van egy bökkenője. Ha a második felhasználó kikapcsolja a számítógépet, akkor az összes olyan fájl elvész, amelyet nem mentettünk el a fiókunkban a felhasználóváltás előtt. Az erre utaló figyelmeztetést könnyű figyelmen kívül hagyni a gyakorlatban.

Az XP a különböző fiókokkal együtt kezeli a *Saját fájlok* mappát, az Asztal nézetét valamennyi ikonnal, így a *Lomtár*-ral, a *Hálózatok-kal,* a *Sajátgép-pel* és a programszimbólumokkal. A Windows XP külön tárolja el a *Kedvenceket,* az Internet Explorer biztonsági beállításait, valamint az Outlook Express postafiókjait. Mindez azt is jelenti, hogy minden felhasználó mindig a saját megszokott környezetét használja, úgy ahogy az Asztalt kialakította.

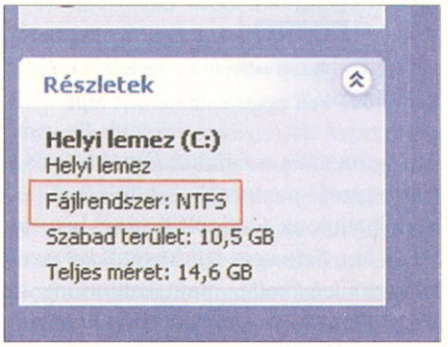
A FAT32 standard fájlrendszer-beállítás esetén, a többi felhasználó számára is betekinthetők maradnak az adatok. Ha megnyitjuk például a *Sajátgép* ikonnal a *C:\Dokumentumok és beállítások* mappát, akkor a többi felhasználó személyes állományait is láthatjuk, sőt módosíthatjuk is.

A felhasználói profilok elkülönítése – legalábbis részben – a telepített programok esetében is elérhető. Az, hogy a Windows csak egy felhasználónak vagy valamennyi fióknak a rendelkezésére bocsát-e egy programot, a szoftver setup rutinjától függ. A kiválasztási opció lehet például az *Igen, a telepítés valamennyi felhasználó számára elérhető legyen.* Kapcsoljuk ki ezt a funkciót, ha csak mi szeretnénk a szoftvert használni.

Nagyobb biztonság: a helyes beállítások

A *Saját fájlok* mappa az Asztalon ugyan rejtve van a többi fiók felhasználója előtt, ám ennek ellenére hozzá lehet férni mások állományaihoz, mi több, nemcsak bele lehet nézni, de szerkeszteni és törölni is lehet. Ezen változtatnunk kell! Nem árt azonban tudni, hogy a Home Edition csak akkor képes a hozzáférés ellen biztonsággal levédeni az adatainkat, ha a modern *NTFS (New Technology File System)* fájlrendszert használjuk.

Először tehát vizsgáljuk meg, hogy NTFS-re lett-e állítva a merevlemezünk, illetve a munkapartíciónk. Kattintsunk duplán a *Sajátgép* szimbólumra, és jelöljük ki a *C:* partíciót. Adott esetben balra az oszlopban aktiválnunk kell a *Részleteket,* hogy az adatok láthatóvá váljanak.



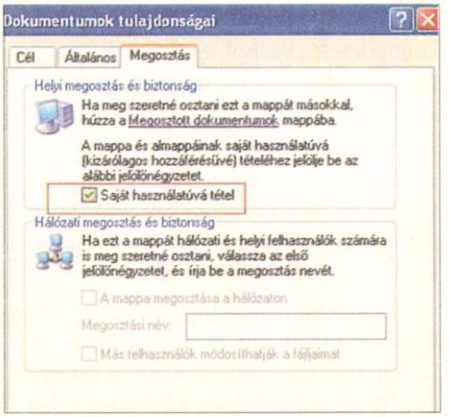
Ellenőrizzük munkapartíciónk fájlrendszerét!

Ha a partíciónk még a FAT32 fájlrendszert használja, akkor állítsuk át NTFS-re. A partíció konvertálásához kattintsunk a *Start* gombra és a *Futtatásra.* A következőket kell begépelnünk: *convert c:/fs:ntfs.* Itt a *C:* betű az első, átállítani kívánt partíciót jelöli. Nyomjuk le az **Enter** gombot. A megjelenő üzenetet nyugtázzuk, és indítsuk újra a gépet.

Amíg a konverzió befejeződik és a gépünk újraindul, eltelik néhány perc. Ismételjük meg az előbbi lépéseket adott esetben egy másik partícióval is, ha kényes adatokat szeretnénk elhelyezni oda.

Egy mappa vagy egy fájl védelméhez a legjobb, ha a teljes mappát kijelöljük a fióknevünkkel a *C:\Dokumentumok és beállítások* alatt, és az egér jobb oldali gombjával megnyitjuk a helyi menüt. Kattintsunk a *Megosztás és biztonság* opcióra, és kattintsunk a *Saját használatúvá tétel* bejegyzésre. Az *OK*-ra kattintva lépjünk ki az ablakból. Ennek hatására a Windows meg fogja tagadni más felhasználó hozzáférését ehhez a mappához, feltéve ha az a felhasználó egy másik fiókon keresztül jelentkezett be az operációs rendszerbe.

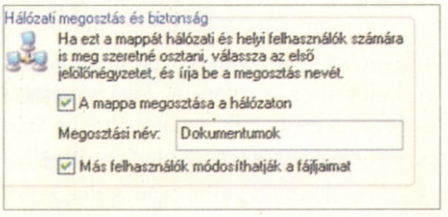
Vegyük figyelembe, hogy a *C:* partícióban csak a felhasználói profilba tartozó



Most már csak mi férünk hozzá a dokumentumainkhoz

mappákat lehet letiltani. Ezek a *Saját fájlok,* az Asztalon lévő mappák és adatok, a *Start menü,* valamint a *Cookies* és a *Kedvencek.* Az összes többi fájl esetében hiányzik a *Megosztás és biztonság* menüpont.

Ha a PC-nk hálózathoz csatlakozik, akkor pontosabban is be lehet állítani a fájlok hozzáférési jogait. Nyissuk meg a megosztani kívánt fájl, illetve a mappa helyi menüjét, majd válasszuk a *Hálózati megosztás és biztonság* opciót.



A hálózatba kapcsolt gépen is megoszthatjuk mappáinkat

A *Megosztás* regiszterlapon kattintsunk *A mappa megosztása a hálózaton* szövegre, s az alatta lévő mezőbe írjunk be egy megosztási nevet, és kapcsoljuk be a *Más felhasználók módosíthatják a fájljaimat* opciót is. Ebben az esetben mások már nemcsak megtekinthetik, de törölhetik vagy szerkeszthetik is a fájlokat. A mappát az *Alkalmaz* paranccsal osztjuk meg.

Felhasználói fiókok a gyakorlatban

A munkahelyi PC esetében, vagy ha több családtag is ugyanazt a számítógépet használja, egyszerű a helyzet. Mindenki a saját fiókjában dolgozik és a bejelentkezési menüvel jelentkezik be, és a legjobb, ha jelszava is van. De még ha egyedül is használjuk a PC-nket, célszerű két fiókot létrehozni a fent említettek szerint. Egy

rendszergazda fiókot kizárólag szerviz és konfigurációs célból, és a korlátozott fiókot, hétköznapi használatra. Ennek az az előnye, hogy ha a gépünket támadás éri az internetről, akkor a hacker mindig csak olyan jogokkal rendelkezik, mint amilyennel a bejelentkezett felhasználó. Egy korlátozott fiók esetében tehát kisebb a lehetséges kár.

Ha mindig a korlátozott fiókon keresztül jelentkezünk be, akkor egy ügyes trükkel átléphetjük a bejelentkezési procedúrát. De az alábbiakban ismertetett lehetőséggel tényleg csak akkor éljünk, ha egyedül használjuk a PC-t.

Kattintsunk a *Start,* majd a *Futtatás* parancsra. Írjuk be a *control userpassword2* utasítást, majd nyugtázzunk *OK*-val.

A következő ablak *Felhasználó* regiszterlapján először jelöljük ki azt a fiókot, amelyen keresztül a Windows a jövőben automatikusan beléptet minket. Ezután kapcsoljuk ki a *Felhasználói név és jelszó megadása szükséges* opciót, és lépjünk ki az *Alkalmaz-zal.*

A következő lépésben kétszer nyugtázzuk a jelszavunkat, és *OK*-val zárjuk le az ablakot. A Windows következő indulásakor automatikusan a Windows Asztal fog megjelenni. A rendszergazda fiókjába való bejutáshoz ezután a legegyszerűbb módszer a gyors felhasználóváltás, a *Start* és a *Kijelentkezés* menüvel.

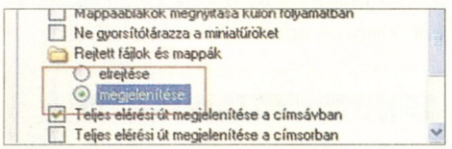
Előzzük meg az adatvesztést!

A különböző felhasználói profilok elkülönítése a gyakorlatban problémamentes, a gondok sokkal inkább a Windows XP további funkcióival adódnak. Ez mindenekelőtt a *rendszer-visszaállításra* vonatkozik. Ennek a segítségével egy lefagyás után egy korábbi, még működőképes állapotába lehet visszaállítani az operációs rendszert. Viszont egy rendszer-visszaállításkor az összes fiók, valamint az azóta eltelt idő alatt készített vagy megváltoztatott személyes fájl törlődik. Ezért rendszeresen mentsük le az e-mailjeinket, a személyes adatainkat, valamint az Internet Explorer Kedvenceket.

Indítsuk el a böngészőt, és a menütárban kattintsunk a *Fájl/Import és export,* valamint a *Kedvencek exportálása* parancsra. Fogadjuk el az alapértelmezéseket, és a lementést fejezzük be a *Befejezésre* kattintva. Az XP a bookmark-fájlokat a *Saját fájlok* mappába másolja át. A cookie-kat ugyanígy kell exportálni.

Az Outlook Express automatikusan a felhasználói profilunkban tárolja el az e-mailjeinket.

Azonban mielőtt dolgozhatnánk vele, előbb láthatóvá kell tennünk a *Helyi beállítások* tárolómappát. Az *Intézőben* a menüsorban az *Eszközök* menüben, a *Mappa beállításai* alatt a *Nézet* regiszterlapon ki kell kapcsolni a *Rejtett fájlok és mappák elrejtése* opciót. Valamivel lejjebb pedig kapcsoljuk be *Rejtett fájlok és mappák megjelenítése* opciót.



Láthatóvá kell tenni valamennyi fájlt

A címeinket a *Fájl,* az *Exportálás* és a *Címjegyzék* parancsok segítségével exportálhatjuk az Outlook Express-ben. Jelöljük ki a *Szöveges fájl (vesszőkkel és elválasztó jelekkel)*-t, majd kattintsunk az *Exportálás*-ra, és könyvtárként hagyjuk meg a *Saját fájlokat.*

A legfontosabb adatok ezzel a felhasználói név alatti *C:\Dokumentumok és beállítások* alá kerültek. Írjuk ki ezeket az adatokat egy CD-re, és jól őrizzük meg. Rendszeres időközönként ismételjük meg a lementést.

Ahhoz, hogy szükség esetén ismét importálni lehessen az adatokat, előbb adott esetben a CD-ről a merevlemez egy tetszőleges helyére kell írnunk a fájlokat. Itt nyissuk meg az egér jobb oldali gombjával ezek helyi menüjét, és válasszuk a *Tulajdonságokat.* Az *Általános* regiszterlapon távolítsuk el a fájl írásvédelmi attribútumát. Ezt követően az Import varázsló segítségével ismét bevihetjük az Outlook Express-be az adatokat.

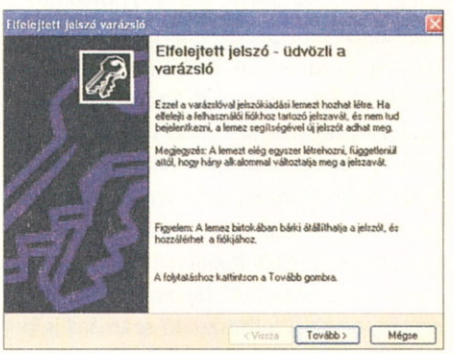
Kizártuk magunkat?

Sokan vannak, akik – hívatlan látogatóktól tartva – jelszóval védik a számítógépüket.Sajnos fenyeget annak a veszélye is, hogy elfelejtjük a jelszavunkat és ezzel kizárjuk saját magunkat. Viszont a Windows meglepő módon nyitva hagy egy kiskaput, amelyen keresztül mindig visszatérhetünk a rendszerbe.

Indítsuk újra a gépünket, és a bootolás alatt tartsuk lenyomva az **F8** billentyűt. A bővített Windows start opciók menüjében nyomjuk le a *Pos 1* billentyűt, mire megjelenik a *Csökkentett üzemmód* opció. Nyomjuk le kétszer az **Enter** gombot, hogy a Windows csökkentett üzemmódban induljon. Most megjelenik egy korábban láthatatlan *Rendszergazda* fiók is. Ez minden védelmet mellőz, nincs levédve jelszóval.

Ennek a biztonsági hiányosságnak a megszüntetéséhez jelentkezzünk be védett üzemmódban ezen a fiókon keresztül, és a *Start/Vezérlőpult/Felhasználói fiókok* parancsokkal nyissuk meg a *Rendszergazda* fiókot. Zárjuk be a bejáratot azzal, hogy a *Jelszó létrehozásával* megadunk egy jelszót. Persze ezzel az utolsó védelem nélküli hozzáférési lehetőséget is bezártuk.

Szerencsére egy második elérési lehetősége is létezik a számítógépnek. Megelőzésképpen készíthetünk egy flopit a jelszavunkkal. Ehhez a rendszergazda jogosultságú fiókba kell bejelentkezni, és a *Vezérlőpulton* keresztül be kell lépnünk a fiókunk „tulajdonságaiba".



Feledékenység ellen: varázsló

A bal oldali oszlopban kattintsunk a *Jelszó elfelejtésének megelőzése-re,* és kövessük a varázsló utasításait. Tegyünk be egy üres flopit, majd nyugtázzunk a *Tovább-bal,* és írjuk be az aktuális jelszót. A Windows ekkor egy úgynevezett *Jelszó-visszaállító* flopit hoz létre. Biztonságosan tároljuk a flopit, mert segítségével bárki hozzáférhet a gépünkhöz.

Ha valamikor elfelejtettük volna a jelszót – még ha időközben meg is változtattuk –, a bejelentkezéshez kattintsunk a képernyőn a fiók mellett jobbra, a zöld nyílra, majd a megjelenő ablakban az *itt* szóra a szövegben.

Helyezzük be a flopit, és írjunk be egy új (!) jelszót. Ismételjük meg ezt a jelszót, majd a következő bejelentkezéskor ezzel ismét hozzáférhetünk a PC-nkhez. ■

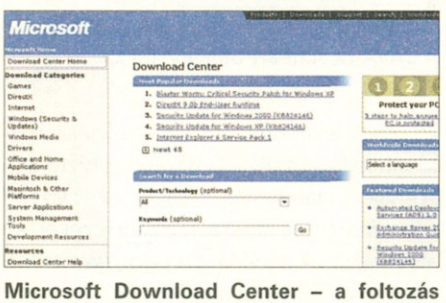
Foltozgatás

Az egyszerűbb vírusok és hackertámadások kapuja sok esetben a böngészőprogram is lehet: célszerű betömni a réseket. Írásunkban ehhez adunk tanácsokat.

A biztonsági szoftverek gyártói rendszeresen figyelmeztetnek az interneten villámgyorsan terjedő új szoftverekre. Időközben számos piackutató intézet felfedezte, hogy ennek ellenére bűnösen elhanyagolják a biztonság kérdését a magánhálózatokon és a számítógépeken. A vállalatok gyakran panaszkodnak olyan behatolásokra a szervereiken, amelyek során bizalmas információkat vagy akár hitelkártya-állományokat másoltak le. Azok viszont, akik az otthoni PC-vel böngésznek, az adatvesztéseket és az emelt díjas telefonszámmal való visszaéléseket emlegetik a leggyakrabban. Pedig az interneten leselkedő veszélyek ellen nem is olyan nehéz védekezni. A nagyobb online biztonsághoz vezető út első lépései az aktuális böngészőverziók és patch-ek, a megfelelő programbeállítások és a hálón való ésszerű viselkedés.

Aktuális programverziók és patch-ek

A Microsoft általában gyorsan reagál a termékeivel kapcsolatos új biztonsági rések felfedezésére. Ha például nyilvánosságra hozzák az Internet Explorer érzékenységét a manipulált HTML-kóddal kapcsolatban, nemsokára megjelenik a Microsoft Download weboldalán egy *Security Update*. A



Microsoft Download Center – a foltozás első lépése

Microsoft úgynevezett *kumulatív patch*-ekként egybe fogja ezeket az update-eket, amelyek az összes megelőző patch-eket is helyettesítik. Az Internet Explorerhez időközben egy *Service Pack* is megjelent. Ha már a böngésző 6.0 verzióját telepítettük, úgy a Service Pack ezt a verziót is aktualizálja. Az Internet Explorer korábbi verzióinál a böngésző teljesen újratelepítődik.

A rendszerünkhöz való alkalmas update-ek megtalálásához lépjünk be a *Microsoft Download Centerébe* a **www.microsoft.com/downloads** címen. A bal oldali oszlopban válasszuk a *Hungarian* bejegyzést. A következő oldal alján a kulcsszó alá írjuk be az *Internet Explorer 6*-ot. Ekkor 12 találatot kapunk. Kattintsunk a legfelső sorban álló legaktuálisabb *Internet Explorer 6 Service Pack 1* bejegyzésre.

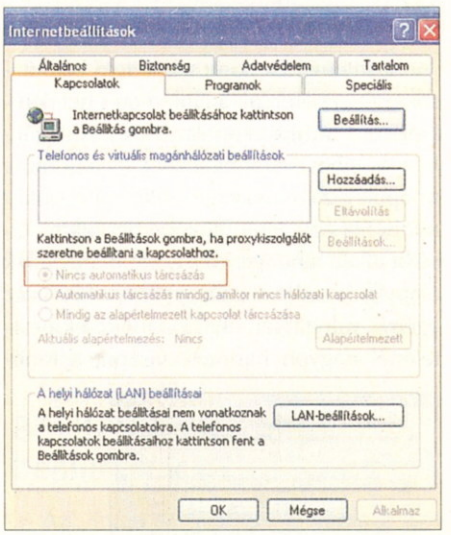
A következő weboldalon találjuk az *ie6setup.exe* webinstaller-t. Miután erre a hozzárendelésre kattintunk, a következő ablakban két lehetőségünk kínálkozik. Vagy rákattintunk a *Megnyitás* kapcsolóra, és azonnal elindítjuk a telepítőt, vagy eltároljuk a fájlt, hogy később végezhessük a Service Pack online telepítését. Az internetes hozzáféréstől és a rendelkezésre álló programverziótól függően az eljárás öt perc és két óra között szokott lezajlani. Az egyes programfájlok tárolási helyével most sem kell foglalkoznunk. Az összes fájl automatikusan felülíródik vagy újjal bővül.

Az automatikus tárcsázás kikapcsolása

Tagadhatatlan, hogy az automatikus internetes tárcsázás kényelmes dolog. Elég valamelyik Windows dokumentumban csak rákattintani egy hozzárendelésre, és máris létrejöhet a kapcsolat az adott honlappal. De az emelet díjas telefonokat üzemeltetők éppen ezt a kényelmet használják ki, és titokban megváltoztatják a telefonos kapcsolati adatainkat. Az ilyen szolgáltatást kínálók úgy okozhatnak aránytalanul nagy telefonköltséget, hogy észre sem vesszük. Az automatikus tárcsázás kikapcsolásával ellenőrizni tudjuk a kapcsolat létrejöttét.

Nyissuk meg a *Start/Beállítások/Vezérlőpult* alatt az *Internetbeállítások-at*. Kattintsunk a *Kapcsolatok* regiszterlapra.

Itt rendszerint aktív a *Mindig az alapértelmezett kapcsolat tárcsázása* opció. Ezzel szemben mi a *Nincs automatikus tárcsázás* opciót válasszuk. A jövőben ennek hatására minden internetes tárcsázás előtt megjelenik a *Telefonos kapcsolat* ablak, amelyben ellenőrizhetjük a standard



Válasszuk a „Nincs automatikus tárcsázás" opciót

szolgáltatónkat és a felhasználói nevünket. Csak ezután adjuk be a jelszavunkat, és kattintsunk a *Tárcsázás* kapcsolóra.

Ne tároljunk el jelszavakat!

Alapvetően ne tároltassuk el a beviteli mezőkben megadott jelszavakat vagy a bizalmas adatokat. Éppen az olyan standard alkalmazások esetében, mint amilyen például az Internet Explorer, könnyű az ilyen eltárolt jelszavak kikémlelése. Az automatikus internetes tárcsázáshoz hasonlóan az eltárolt jelszó is meggyorsítja a tárcsázást, de egyben növeli a biztonsági kockázatot. Ezért inkább válasszuk a bonyolultabb utat, és minden alkalommal adjunk meg külön a jelszót.

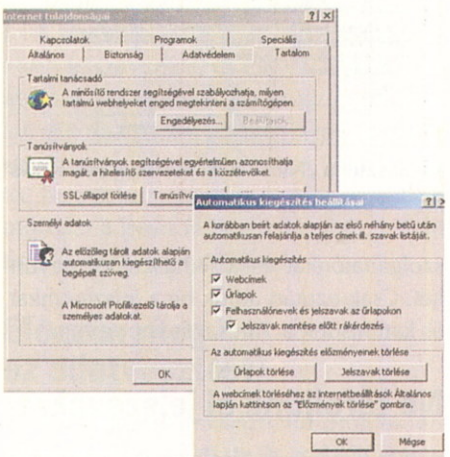
Ha a telefonos kapcsolathoz tartozó jelszavunkat már eltároltuk, akkor ismét töröljük ki. Ehhez válasszuk a *Start/Beállítások/Vezérlőpult* alatt az *Internetbeállításokat*, és válasszuk a *Kapcsolatok* regiszterlapot.

A *Telefonos kapcsolatok* listából válasszuk ki az egérrel a standard szolgáltatón-

kat, és kattintsunk a *Beállítások* kapcsolóra. A következő ablak alsó harmadában töröljük a *Jelszó* mögötti bejegyzést, majd nyugtázzunk *OK*-val. Mielőtt tehát a hálózattal felvennénk a telefonos kapcsolatot, megjelenik a jól ismert *Telefonos kapcsolat* ablak. Ebben meg kell adnunk a jelszavunkat, és a *Tárcsázás* kapcsolóval kell nyugtáznunk. Győződjünk meg róla, hogy a *Jelszó mentése* opció nincs kijelölve.

A beviteli támogatások kikapcsolása

Az Internet Explorer megfelelő beállítások esetén nemcsak az internetes bejelentkezéshez tárolja el a jelszót. A webcímekhez, a felhasználói nevekhez és az online űrlapokhoz úgynevezett *online támogatást* nyújt. Ha egy ilyen mezőbe beírjuk az első betűket, a böngésző a korábbi bevitelek alapján javaslatot tesz, amelyek közül az egérrel válogathatunk. Ez az URL-ek bevitelénél nagyon hasznos, viszont a rend-



Hasznos funkció – de vajon biztonságos is?

szerünk biztonsága érdekében mondjunk le a beviteli támogatásról az űrlapmezők és a jelszavak esetében.

Nyissuk meg a *Start/Beállítások/Vezérlőpult* alatt kettős kattintással az *Internetbeállításokat,* majd lépjünk be a *Tartalom* regiszterlapra. Kattintsunk az *Automatikus kiegészítés* kapcsolóra.

A következő ablakban csak a *Webcímek* kijelölését hagyjuk meg, hogy az URL-eknél azért élvezhessük az automatikus kiegészítés előnyeit. Ezzel szemben kapcsoljuk ki a beviteli támogatást az *Űrlapok* és a *Felhasználónevek és jelszavak az űrlapon* esetében. A már eltárolt adatok törléséhez kattintsunk az *Űrlapok törlése* és a *Jelszó törlése* kapcsolókra.

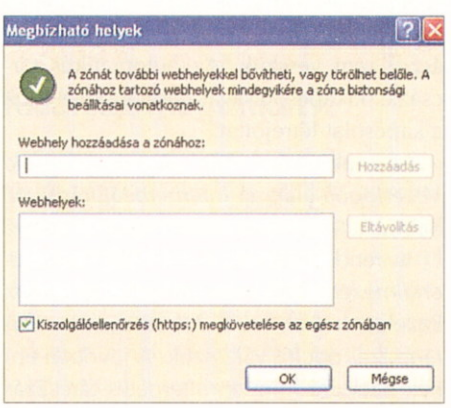
A biztonsági fokozatok helyes beállítása

A Windows négy zónára osztja fel a hálózatokat: *Internet, Helyi intranet, Megbízható helyek* és *Tiltott helyek.* Az Internet Explorerrel meghatározhatjuk minden

A Windows négy biztonsági zónát határozott meg

egyes zóna biztonsági szintjét, ami az alacsonytól a *magasig* terjedhet. Itt is érvényes, hogy a magas biztonsági szint a legnagyobb védelmet kínálja, de egyúttal a böngészést is korlátozza, így például nem jelennek meg az animált elemek. Ezért érdemes először valamelyik közepes biztonsági szintet kiválasztani, és később kézzel kiegészíteni az ebből eredő beállításokat.

Nyissuk meg a *Start/Beállítások/Vezérlőpult* alatt az *Internetbeállításokt,* majd aktiváljuk a *Biztonság* regiszterlapot. Az *Internet* mint tartalmi zóna alapértelmezésként már ki van jelölve. A *Helyi intranet*re csak egy cég belső weboldalai



Jól gondoljuk meg, milyen webcímet nyilvánítunk megbízható helynek

esetében van szükség. A *Megbízható helyek*nél olyan weboldalakat adjunk meg, amelyeket a beállított biztonsági fokozattól függetlenül, korlátlanul szeretnénk meghívni. Ezzel szemben például egy alacsony biztonsági fokozatnál olyan lapokat definiálunk, amelyeket bizonytalanként értékelünk, és ezekhez a *Tiltott helyekhez* magasra kell állítanunk a tológombot.

Kattintsunk az egér bal oldali gombjával a tológombra, és lenyomva tartott gombbal mozgassuk el azt. A szabályozóelem mellett jobbra megjelennek a biztonsági szintek, és ezek hatásának ismertetése a böngészésre és a letöltésekre. Javasolt a *Közepes* beállítás. Az eljárást szükség esetén ismételjük meg a másik három zóna esetében is. Az *OK*-ra, majd az *Alkalmaz*-ra kattintva nyugtázzunk.

A scripting ellenőrzése és kikapcsolása

A Java-Appletek mára számos weboldalon szabványosnak számítanak. Ezek gondoskodnak például a tőzsdei diagramok aktualizálásáról, vagy arról, hogy a böngésző ablakában kis játékokat online

A JAVA-ra sem árt odafigyelni kicsit

lehessen lejátszani. A Java-Appletek önálló miniprogramok, és viszonylag biztonságosnak számítanak, mert a *Virtual Machine (VM)* játssza le őket. Ezeket az alkalmazásokat például a **http://java.sun.com** weblapról tölthetjük le. A Java-Applet-ekkel ellentétben a *JavaScriptek* könnyen kikémlelhetik és manipulálhatják a számítógépünket. A JavaScript egy makrónyelv, és a böngészőnk közvetlenül futtatja. Például az online banking esetében ilyen JavaScriptek ellenőrzik a beadott számlaadatokat.

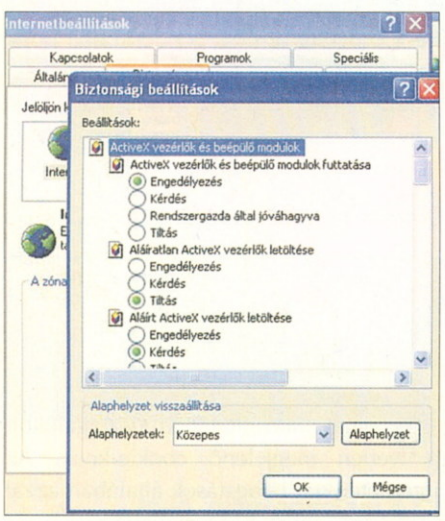
A script-folyamatok biztonságának a növeléséhez aktiváljuk az *Internetbeállítások* alatt a *Biztonság* regiszterlapot, ahol az imént a *közepes* biztonsági szin-

tet állítottuk be. Kattintsunk most az *Egyéni szint* kapcsolóra. A *Beállítások* ablakot görgessük le a *Parancsfájlkezelésig*. Ideális megoldás, ha az *Active scripting* alatt bekapcsoljuk a *Kérdés* opciót. Ezzel a jövőben minden scriptet tartalmazó weboldal esetében egy üzenet jelenik meg, és magunk dönthetjük el, hogy megengedjük-e (megbízható oldalakon) vagy letiltjuk-e (a kétes oldalakon) a scriptet.

Ez a beállítás azonban feltehetően hamarosan terhessé fog válni, hiszen alig létezik már script nélküli weboldal. Ekkor az *Active scripting* alatt kattintsunk az *Engedélyezésre*. Viszont *A beillesztés műveletének engedélyezése parancsfájlokon keresztül* és a *Java kisalkalmazások hívása parancsfájlból* opciókat minden esetben le kell tiltanunk!

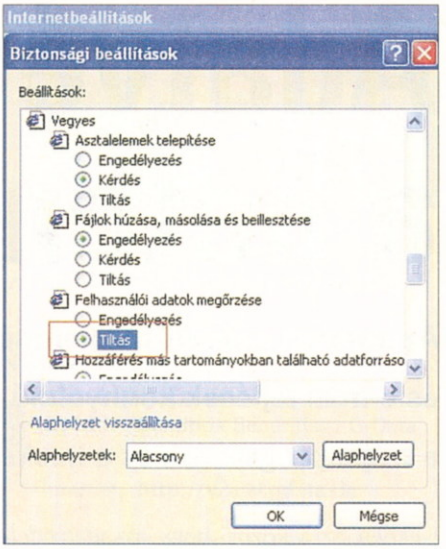
Az ActiveX kikapcsolása

Az ActiveX komponensek olyan vezérlőelemek, amelyeket webalkalmazásokhoz fejlesztett ki a Microsoft, s a Java-Applet-ekhez hasonlóan interaktív alkotókat szerkesztenek be az oldalakra. Ezekkel ellentétben viszont sokkal könnyebb visszaélni velük. Mivel az ActiveX komponensek nem olyan elterjedtek, mint a JavaScriptek, sokkal könnyebben ellenőrizhetők vagy teljesen ki is kapcsolhatók.



Itt szabályozhatjuk az ActiveX vezérlők viselkedését

Ismét az *Internetes beállítások Biztonság* regiszterlapjára lesz szükségünk. Kattintsunk az *Egyéni szint* kapcsolóra. A *Biztonságosként megjelölt ActiveX vezérlők futtatása* és az *ActiveX vezérlők és beépülő modulok futtatása*, valamint az *Aláírt ActiveX vezérlők letöltése* opciókhoz válasszuk a *Kérdés* lehetőséget. Az aláíratlan és a nem biztonságosként megjelölt ActiveX vezérlőelemek esetében természetesen a *Tiltás* opciót kell választanunk.

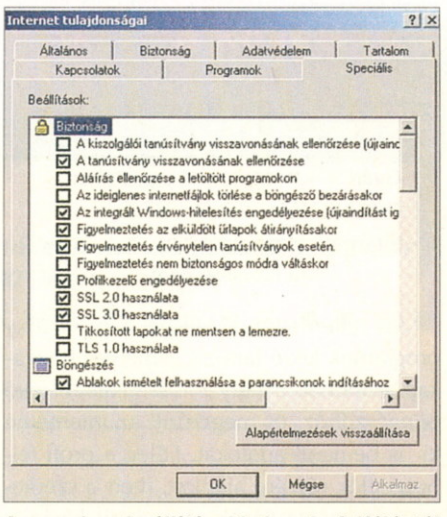


Ne engedjük megőrizni a felhasználói adatokat!

A felhasználói adatok tárolásának megtiltása

A Microsoft a *Vegyes* rovatban néhány további biztonsági beállítást gyűjtött össze, amelyeken a *Közepes* biztonsági szintről kiindulva javíthatunk. A legtöbb a *Kérdés* opcióra lett beállítva, így a böngészés során informálódhatunk a biztonsági szempontból lényeges folyamatokról. De ha egészen biztosra akarunk menni, és mindenütt a *Tiltást* kapcsoljuk be, akkor ez feltehetőleg semmilyen hatással sem lesz a böngészésre.

Nyissuk meg az *Internetbeállítások*



A gondos beállításokkal sok fejfájástól kímélhetjük meg magunkat

El a profilokkal!

Jobb, ha nem aktiváljuk a *Profilkezelő engedélyezését*. A varázslót az *Internetbeállítások* alatt, a *Tartalom* regiszterlapon és a *Saját profil* kapcsolóval definiálhatjuk. Ehhez, személyes adatokat kell megadnunk. A honlapok üzemeltetői ezután hozzáférhetnek ehhez a profilhoz, és személyre szabott ajánlatokat állíthatnak össze. Ez az eljárás ugyan nem kívánatos, viszont alig akad honlap, ahol ezt használják.

alatt a *Biztonság* regiszterlapot. Kattintsunk az *Egyéni szint* kapcsolóra, és a *Beállítások* ablakban menjünk le a *Vegyes* rovatig.

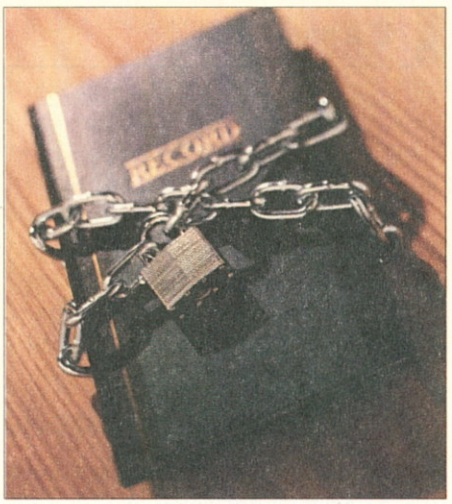
A bejegyzések a weboldalak értelmezésének számos különleges esetét érintik. A második helyen a *Felhasználói adatok megőrzése* bejegyzés áll. Ezt a már ismertetett okokból, a bevitelünk biztonsága érdekében le kell tiltani.

Bővített biztonsági beállítások

Az Internet Explorer biztonságával kapcsolatban néhány további beállítást találhatunk az *Internetbeállítások* menü *Speciális* regiszterlapján. Itt lényegében az aláírással vagy a kódolási mechanizmusokkal védett internetes oldalak kezeléséről van szó. Az Internet Explorer 6-os verziójában egyébként már eltávolították a feleslegesnek tartott bejegyzéseket, mint például a *Frontezza* kódolást. Ezért – kettő kivételével – a rovat összes opcióját kapcsoljuk be.

Egy weboldal betöltésekor az oldal alkotóelemei, például a képek, a rajzok, a szövegek stb., egy átmeneti mappában tárolódnak el. *Az ideiglenes Internetfájlok törlése a böngésző bezárásakor* opció hatására ezek az alkotóelemek kompletten kitörlődnek, miután kilépünk az internetből.

Ennek a megoldásnak az az előnye, hogy nem lehet olyan könnyen kifürkészni böngészési jellemzőinket. Másfelől viszont a rendszeresen felkeresett honlapokat mindig újra teljesen le kell tölteni. Ezt lassú kapcsolatok esetén, például modemes hozzáférésnél, célszerű meggondolni. A gyors kapcsolati lehetőségeknél mindenképpen túlsúlyban vannak a törlés előnyei. ■



Adatvédelem a neten

Az internet számos meglepetést tartogat: a cache-ek, cookie-k és e-mail fejlécek könnyelmű kezelésének eredményei a trójai programok és a hackerek külső támadásai.

Internetes kapcsolatunk biztonságáért magunk is sokat tehetnénk. Sokszor azonban kevés az idő, hogy megismerjük a böngészők és a levelezőprogramok apróbb, de annál fontosabb részleteit. Az alábbiakban tüzetesebben bemutatunk több ismert shareware-et és ingyenes programot, amelyek mind-mind a biztonságunkat erősítik.

Védőszoftverek

Feltehetően sokan tudják, hogyan lehet kiüríteni a böngészőtárat, hogyan lehet törölni a meglátogatott weboldalak listáját, hogyan lehet maradéktalanul eltávolítani a „sütiket". A böngészőprogramok olyan funkciókat és beállításokat is kínálnak, amelyek megakadályozzák a cookie-k felírását. Ez azonban nem mindig kívánatos. Internetes vásárlás esetén a cookie-kat arra használják, hogy a bevásárlókosár aktuális tartalmát mutassák. Amennyiben a vásárló az árut belehelyezte a bevásárlókosárba, de a kapcsolat valami miatt megszakadt, a következő alkalommal nem kell mindent elölről kezdeni, a lista a legutóbbi állapotot mutatja. Ha a cookie-kat előzőleg kitiltottuk a böngészőből, most ismét elindulhat a hajsza az ajánlatok után. Valójában tehát szükségünk lenne egy olyan programra, amely *először kiüríti a mappákat, majd külön választja a lényegest a „szeméttől"*.

Az, hogy a böngészőkből pontosan milyen adatok jutnak el egy harmadik személyhez, attól is függ, hogyan konfiguráltuk a programot. De hogyan jegyezzünk meg ennyi beállítást? Jó lenne egy olyan program, amely figyeli a böngészőt. A továbbiakban különböző felhasználási területek programjait mutatjuk be, amelyekben az a közös, hogy *az adatvédelmet szolgálják az interneten.*

Steganos

Gyártó: DEMCOM
Feltétel: Windows 9x, ME, NT 4.0 és 2000, Explorer 6 és Netscape Communicator 6-
Internet: **www.steganos.com/de**

Az internetes nyommegsemmisítő, amely eddig a *DEMCOM Steganos 3 Security Suite* szoftveres csomag része volt, immár önállóan is kapható. A program kiüríti a böngésző mappáját, amely tárolja az addig behívott oldalakat (*History*), valamint törli a tárakat, és a kapcsolat felvétele után kitiltja a böngészőből a cookie adattárolókat. A külön beépített *Shredder* pedig arról gondoskodik, hogy az adatokból semmi se maradjon meg olvasható formában. *A programot az Internet Explorer 6-os verziójával és a Netscape Communicator 6-tal lehet használni.*

Internet Junkbuster

Gyártó: Junkbuster Corporation
Feltétel: Windows 9x, NT 4.0
Internet: **http://internet.junkbuster.com/**

Az *Internet Junkbuster* azon proxy programok közé tartozik, amelyek hozzákapcsolódnak a helyi, használatban levő böngészőhöz, és megszűrik az interneten ki- is bemenő adatokat. Főleg a profi felhasználók részére ajánlott, mert a szerkezete olyan utasítások megadását kívánja, amelyek bizonyos operációkat hajtanak végre a kapcsolat alatt. Az utasításokat a program egy elkülönített INI adattárban gyűjti össze, amelyet a program az indítás után leolvas, majd alapul vesz a műveletek elvégzéséhez. Ide tartozik a hirdetési csíkok, illetve a reklámlevelek blokkolása, de a program arról is gondoskodik, hogy az adatok alapján ne lehessen következtetni a felhasználó személyére, vagy vele kapcsolatos információkhoz jutni.

Cookie-Server

Gyártó: Newfangled Software
Feltétel: Win 9x, ME, 2000
Internet: **www.newfangled.san-jose.ca.us/**

A felhasználó általában kiszolgáltatott a weben megjelenő cookie-knak. Az interneten tett látogatások általában azzal végződnek, hogy néhány újabb bejegyzés található a cookie-listán. Nos, a *Cookie-Server* arról gondoskodik, hogy a felhasználó bosszút állhasson. A program a kapcsolatfelvétellel párhuzamosan indul el, és figyeli, hogy mi zajlik a szerver és a cookie mappa között. Amennyiben a webszerverek valamelyike megpróbálkozik egy cookie-val, a programmal találja szemben magát. Az opciókban be lehet

állítani, hogy milyen módon lehessen megtekinteni a weboldalakat: a cookie-kat ki lehet töröltetni, vagy át lehet vizsgáltatni, anélkül, hogy ezt a webszerver „észrevenné". A program úgy viselkedik, mint egy apró tűzfal.

CT Cookie Spy

Gyártó: Jerry Campbell, Camtech 2000
Feltétel: Windows 9x
Internet: **http://camtech2000.net**

A cookie-k nem mindig az ellenségeink. Vannak azonban cégek, amelyek arra használják azokat, hogy a segítségükkel figyeljék, illetve befolyásolják a felhasználó internetes viselkedését. Ezért kell megvizsgálni a cookie-k tartalmát és azt, hogy pontosan honnan származnak. A *Cookie Spy* átvizsgálja a cookie mappát, megmutat minden benne elhelyezkedő bejegyzést, lehetővé teszi a közvetlen kapcsolat felvételét a cookie gyártójával, és abban is segít, hogy speciális cookie-adatokra leljünk. Például arról is tudomást lehet szerezni, hogy pontosan mennyi információval rendelkezik rólunk egy-egy weboldal.

Secure 4U

Gyártó: Sandbox Securities / G-Data
Feltétel: Win 9x, ME, 2000, NT, 4.0
Internet: **http://www.gdata.de**

Aki átfogó védelemre vágyik, annak érdemes megnéznie a *Sandbox Securities-től* származó *Secure 4U*-t, amely célzottan hárítja el a támadásokat. Kívánságra minden alkalmazást körbezár egy virtuális védődobozzal, amely egyetlen bejárattal rendelkezik. Ez alkotja az egyetlen kapcsolatot a szoftver és a külvilág között. A felhasználó teljes uralmat élvez a Secure 4U felett. A teljes programcsomag, amelyben még egy vírusfigyelő is van, abban segít, hogy megvédjük a személyes adatainkat, a jelszavakat vagy a felhasználóneveket.

WebWasher

Gyártó: Webwasher Inc.
Feltétel: Win 9x, NT, ME, 2000
Internet: **www.webwasher.com**

A *WebWasher* átfogó védelmet nyújt programrészek, például az *ActivX*, vagy adatok, így a céges hálózatokhoz tartozó cookie-k, ellen. A program szűrőként működik, de annál jóval egyszerűbben installálható. Nemcsak az adatokat szűri meg, hanem a hirdetési csíkokat is blokkolja. Az olyan webtartalmak, amelyek a szűrőlistákon szerepelnek, esélytelenek a WebWasherrel szemben. A program főként hálózatba kötött gépek esetén hasznos, de önálló számítógépekre is telepíthető, ha szeretnénk figyelemmel kísérni az azon folyó eseményeket. A programot proxyszerverként is be lehet vetni. ■

Védelem mindenkinek

A mai tűzfalprogramok már szinte kivétel nélkül képesek bezárni a portokat. Persze az erősségüket és a gyengéjüket akkor árulják el igazán, amikor egy hackertámadás éri őket. Lássuk, hogy ki, mit kínál a biztonság területén.

Az esélyt a behatolásra *a Windowsba épített hálózati szolgáltatások, az állomány- és nyomtatómegosztás biztonsági rései* adják. Ezek lehetővé teszik, hogy egy hálózaton belül mások számára is hozzáférhetővé váljanak az erőforrásaink. Amikor azonban az internetre kapcsolódunk, olyanok is bekukkanthatnak merevlemezünk tartalmába, akiknek ezt semmi szín alatt nem óhajtjuk megengedni.

Szkennelőprogramokkal mihaszna emberek állandóan vizslatják a netet olyan számítógépek után kutatva, amelyek nem alkalmaznak védelmet a behatolással szemben. Akik már telepítettek tűzfalat, tapasztalhatták, hogy szörfölés közben milyen sokszor éri támadás a gépüket, a program ugyanis minden kísérletet jelez. Minél több időt töltünk a neten, annál nagyobb a valószínűsége, hogy ránk találnak, és ha nem védjük magunkat egy tűzfallal, nem is fogjuk soha megtudni, hogy valaki kutakodott a gépünkön.

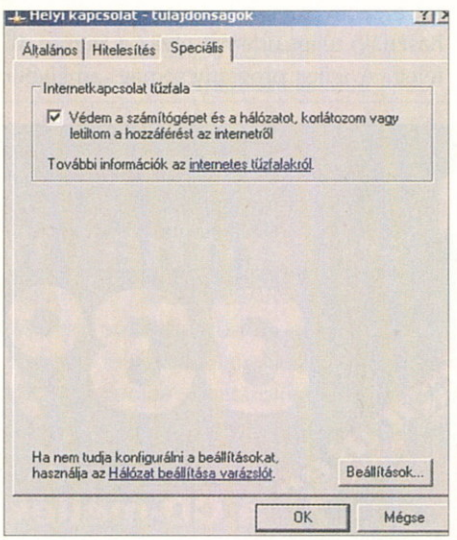
Persze nem csupán kívülről fenyegeti veszély a gépünket: egy trójai program vagy valami más rosszindulatú alkalmazás a megkérdezésünk nélkül szolgáltathat információkat megbízója számára. A jó tűzfal ezt is megakadályozza.

Számos tűzfal víruskeresőkkel együtt érkezik. Ez nem mindig számít jó üzletnek, mert egy olcsó tűzfallal és egy freeware szkennerrel gyakran jobban járunk. Ha azonban amúgy is akartunk vírusszkennert vásárolni, akkor célszerű csomagban megvenni a tűzfallal együtt.

Véd a Windows XP

A *Windows XP* megjelenése óta egy *operációsrendszer-tűzfal* is létezik. Ezzel nemcsak a céges munkaállomásnak szánt professzionális verziót erősítették meg, hanem az otthoni Windowsnak is a részévé vált.

Kattintsunk a *Start/Vezérlőpult* menüben a *Hálózati kapcsolatok* modulra. Itt hívjuk elő az egér jobb oldali gombjával a *Helyi kapcsolatunk* szimbólumot, és válasszuk a *Tulajdonságokat*. A *Speciális* regiszterlapon jelöljük ki az *Internet kapcsolat tűzfalát*, és ettől kezdve már védelem alatt szörfözhetünk. Persze ezzel még nem érezhetjük túl nagy biztonságban magunkat, mert sajnos az XP-tűzfal nem sokat tud. Az egyik nagy gyengéje például, hogy nem foglalkozik az olyan programokkal, amelyek a számítógépünkről kívánnak kapcsolatot létesíteni az internettel. Az ingyenes Microsoft termék tehát nem károsította különösebben a tűzfalkészítőket, még a freeware termékek is többet tudnak nála. Egyes segédprogramok az adatcsomagok szűrésén kívül képesek veszélyes scripteket keresni a weblapok tartalmán, cookie-kat menedzselni, reklámokat kiszűrni és teljes oldalakat letiltani a gyerekek vagy a böngésző kollégák elől.



A Windows XP-nek saját tűzfala van

Hogyan működik?

A tűzfal beépül a számítógép és az internet közé, teljesen elszigetelve őket egymástól. Minden egyes bejövő és kimenő adatcsomagot megvizsgál, majd határoz az átengedésükről, illetve a blokkolásukról. Természetesen mindezt úgy valósítja meg, hogy a normál szörfözést nem teszi lehetetlenné folytonos akadékoskodással, ugyanakkor mindig figyelmeztet a jogosulatlan behatolásra. Arra is kapható, hogy meghatározott IP-címekről teljesen blokkolja az adatforgalmat, illetve csak egy adott webkiszolgálóval engedélyezze a kapcsolatot létesítését.

Magától értetődően bármely tűzfal használatának csak akkor van értelme, ha az minden biztonsági lyukat betöm, vagyis mindkét irányban megakadályoz mindenféle jogosulatlan adatforgalmat. A külső behatolásokkal szemben úgy nyújt védelmet, hogy a kapcsolódásra használatos portokat – és így magát az internetre kapcsolt számítógépet is – láthatatlanná teszi a külvilág számára. A belülről kifelé irányuló adatátviteli próbálkozásokat pedig jelzi számunkra, és mi eldönthetjük, hogy mely programoknak engedélyezzük az adatforgalmazást (ezek közé tartozik például a webböngészőnk és a levelezőprogramunk).

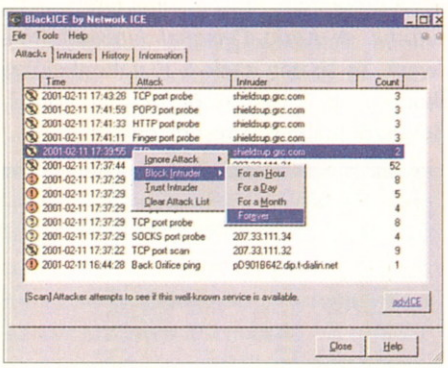
BlackICE Defender 2.1

A *BlackICE Defender 2.1* valójában nem tűzfalprogram, hanem *Instruction Detection System (IDS)*. Négy biztonsági fokozatban vizsgálja a bejövő forgalmat, és a NetBIOS Filesharing problémával is foglalkozik.

A BlackICE biztonsági modellje a rendszer- és alkalmazási portok megkülönböztetésében rejlik. A rendszerportok száma 0-tól 1023-ig terjed, valamennyi magasabb portszám alkalmazási porthoz tartozik. A program a beállított biztonsági fokozattól függően vizsgálja a rendszerportokat, az alkalmazási portokat vagy mind-

kettőt, de mindig csak a bejövő forgalom portjai érintettek. Ez azt jelenti, hogy a „honvágyas" programokat, így például a trójai falovakat nem ismeri fel! Tehát eleve nem szűri az internetre menő forgalmat.

A program igazi erőssége a támadások felismerése. A BlackICE Defender felkutatja a betolakodókat, az IP-címmel NS-lookup-lekérdezést hajt végre, és megjeleníti a megtalált nevet. Erről néha már fel lehet ismerni, hogy a betolakodó telefonos modemről, egy adott tartományból vagy országból jött-e.



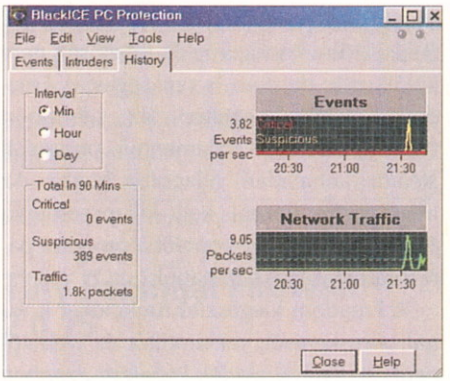
A BlackICE Defender kilistázza a támadásokat

Az IDS egy támadásablakban listázza ki a felismert támadásokat. Így egy bejegyzés helyi menüjében is le lehet tiltani egy támadót. Ha egy támadást kijelöltünk, akkor a program az *advICE* kapcsolóval megjelenít egy weblapot, a támadás típusának információival. A BlackICE angol nyelvű dokumentációja is mintaszerű, valamennyi vizsgált termék közül a legrészletesebb.

További infók: www.networkice.com

BlackIce PC Protection 3.5

A 6 Mbájtos fájlméret robusztus programot sejtet, s bár egy egyszerű kis ablak tűnik fel a képernyőn, a menükben rengeteg beállítási lehetőségre bukkanunk. Mit sem ér azonban a sok sallang, ha a védelem komoly hiányosságokat mutat. Négy biztonsági szint közül választhatunk, de a tesztelés során még a legmagasabb szint beállításával sem tudtuk elérni, hogy gépünk teljesen láthatatlan legyen a külvilág számára. Telepítéskor a *BlackIce* alkalmazásvédelem címén összegyűjti a merevlemezünkön található valamennyi programállományt, aminek az eredménye egy kilométeres lista. A listán szereplő programoknál egyenként kell megtiltani, hogy



A hátbatámadások ellen sajnos nem nyújt védelmet a BlackIce PC Protection

kapcsolatba lépjenek az internettel. Ha ezt nem tesszük meg, a telepítéskor már a gépünkön lévő valamennyi program háborítatlanul küldözgethet adatokat a külvilág felé. Így természetesen a kimenő oldali védelem tesztelésére használt *leaktest.exe* gond nélkül áthatolt a tűzfalon. A súgó tanulmányozásakor kiderült, hogy a BlackIce külön utasítás hiányában csupán a telepítése után rendszerbe kerülő vagy megváltozó programokat blokkolja. Amikor azonban ilyennel próbálkoztunk, a védelem akkor sem működött.

A letölthető program 30 napig használható, utána fizetni kell érte, de a legjobban akkor járunk vele, ha egyáltalán nem telepítjük, mert az ismeretlen alkalmazások ellen nem nyújt védelmet.

További infók: www.iss.net

eSafe Desktop 3.0

Az *eSafe Desktop* voltaképpen egy átfogó biztonsági program, és a vírusok, trójai falovak, kéretlen scriptek ellen is véd. Így már érthető, hogy a program egy vírusszkennelőt és egy sandboxot, valamint egy rendszermonitort is tartalmaz, bizonyos fájlok változtatásainak a követésére.

A biztonsági elv alapját a *sandbox-technológia* képezi. Mindegyik programhoz egy sandboxot lehet definiálni, amely meghatározza, hogy mit szabad a programnak, mely mappákhoz, hogyan férhet hozzá. A program nem léphet ki a sandboxból, így egy veszélyes kód, megfelelő konfigurálás esetén, nem okozhat kárt.

A program *desktop-firewall* modulja a portok felhasználását ellenőrzi. Ehhez különböző előre definiált készleteket használ, amelyek valójában portkorlátozások. A *Trojan Hackers Ports* készlet például olyan portokat tartalmaz, amelyeket előszeretettel használnak a trójai programok, s azok ebben a készletben inaktívak. Persze saját készleteket is definiálhatunk. A készletek szabályokat tartalmaznak, amelyek a port felhasználásáról rendelkeznek. A porton bonyolódó adatforgalmat a szabály minden portjához egyenként lehet beállítani. Ez lehet bejövő, kimenő, vagy kétirányú. Ezt a portot ki vagy be lehet kapcsolni. Mindegyik szabályhoz létezik kivétel is. Ezek olyan hostok, amelyekre a szabály nem vonatkozik. A hostokat a nevükkel vagy az IP-címükkel lehet megadni.

Az *Application-Firewall* modul a telepített programok internetes hozzáférésére felügyel. Hozzáféréssel csak az olyan internetes programok rendelkeznek, amelyek egy előre definiált sandboxban helyezkednek el. Ha egy másik program szeretne internetes kapcsolatot létesíteni, akkor lép a színre a modul, és csak az engedélyezés után valósulhat meg a hozzáférés. Az eSafe-nek nincsenek további tűzfal funkciói, viszont van egy tartalomszűrője. Ez tiltott szavak után keresve végigböngészi az e-mail-címeket, valamint a hírcsoportneveket és fájltartalmakat. A készlet egy tiltott szavakat tartalmazó listából áll. Az előre definiált listák olyan témákat tartalmaznak, mint például hackerek, rasszizmus vagy drogok. A másik jellegzetesség a definiálható karaktersorozatok kódolása. Megadhatunk egy hitelkártyaszámot, s ezt minden alkalommal kódolhatjuk, amikor az interneten továbbítjuk.

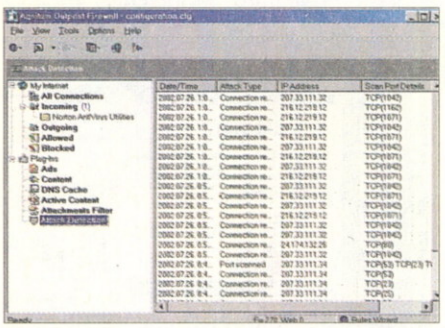
Az eSafe sandboxa meghatározza, hogy egy program hogyan érheti el a mappákat és mely fájlokat futtathatja

További infók: www.esafe.com

Outpost Firewall 1.0

A program különlegességét az adja, hogy bedolgozók (plug-in-ek) készíthetők hozzá, így bárki kiterjesztheti a képessé-

geit. Szolgáltatásai egy részét (így például a levélmelléklet-szűrést és a hirdetésblokkolást) már most is bedolgozók valósítják meg. A Windows Intézőjére emlékeztető barátságos programfelületen könnyen megtalálhatók a szolgáltatások és a beállítási lehetőségek, akár a menüket, akár az eszköztárat használjuk. Szinte nem is kell változtatni a biztonsági konfiguráción: az alapbeállítások a legtöbb felhasználó számára úgy jók, ahogy vannak. Figyelemre méltók a testre szabási lehetőségek is: tág határok között változtatható, hogy a program milyen információkat jelenítsen meg az adatátvitelről, a behatolási kísérletekről, az átengedett és a blokkolt adatcsomagokról, a meglátogatott webhelyekről.



Otthonosan mozoghatunk az Outpost Intéző-szerű felületén

Többnyelvű program lévén telepítéskor az angol mellett más nyelveket is felkínál. A magyar egyelőre nincs a lehetőségek között, ami azért különös, mert a gyártó webhelyéről egy pdf formátumú, magyar nyelvű dokumentáció is letölthető, amelynek képernyő-illusztrációi magyar nyelvűek.

Ötféle biztonsági szint közül választhatunk, az internetezésre használt programok pedig három kategóriába sorolhatók (megbízhatók, blokkoltak és szabály alapján szűrtek). A tesztelés során teljes védelmet nyújtó, 2,7 Mbájtos letöltési méretű Outpost használata ingyenes.

További infók: www.agnitum.com

Freedom Security & Privacy Suite 3.2

A *Freedom-nál* a PC-nken futó valamennyi alkalmazáshoz külön definiálhatjuk, hogy hozzáférhet-e az internethez vagy sem, hogy működhet-e szerverként, és hogy minden kapcsolatfelvétel előtt előbb kérdeznie kell-e. A felhasználó ezen kívül általánosan, vagyis együttesen ki- és bekapcsolhatja a protokollokat. Sokkal több konfigurációs lehetőség nem kínálkozik, de nem is szükséges. A Freedom alapértelmezetten az Ident-port (113) kivételével valamennyi portunkat *stealth* (láthatatlan) állapotba hozza. Az Ident-portot kézzel kell kikapcsolnunk. Az ehhez szükséges opciót a program paraméterezésénél találhatjuk.

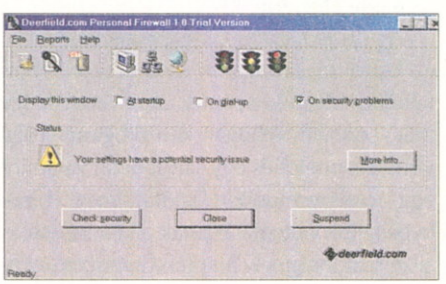
A Freedom kiegészítő funkciókat is kínál: víruskeresőt, reklámtiltót és weblapcenzort. Ezen funkciók kezelése azonban kissé nehézkes, a felhasználónak kézzel kell elkészítenie a tiltott weblapok vagy címszavak jegyzékét.

Összegzésként elmondható, hogy a Freedom alapvédelmet nyújt az egymunkahelyes PC-knek, ám nem összetett feladatokra készült.

További infók: www.freedom.net/products

Personal Firewall 1.0

Egyszerű felépítésű program, a szolgáltatásai közvetlenül elérhetők az eszköztárról. Az alapbeállításai megbízható védelmet nyújtanak mindkét irányban. A szokásos három biztonsági szinthez – a teljes blokkoláshoz, a szabály alapú normál üzemmódhoz és a mindennemű adatforgalom átengedéséhez – egy-egy közlekedési jelzőlámpa tartozik, így pofonegyszerű az átkapcsolás közöttük. Külön biztonsági beállításokat alkalmazhatunk az otthoni, az irodai és a mobil használatra, s ugyancsak ikonokra való kattintással választhatunk e profilok közül.



A Personal Firewall egérkattintásokkal vezérelhető

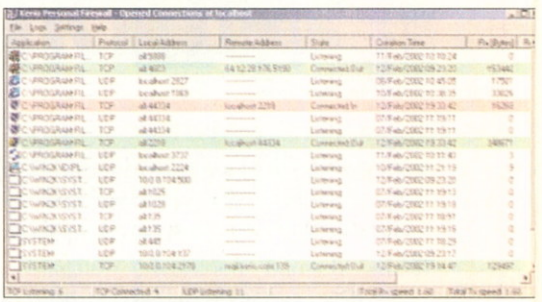
Telepítés után az 1,4 Mbájtos *Personal Firewall* biztonsági ellenőrzést hajt végre a gépünkön (ezt később bármikor megismételhetjük), az alkalmazások listájára felveszi azokat az internetezésre használatos programokat, amelyeket a rendszerben talál, és a biztonságos működéshez szükséges szabályokat alkot hozzájuk. A további programokhoz való szabályalkotás azonban eléggé macerás, és csak tapasztaltabb felhasználóknak ajánlott. Más személyi tűzfalaknál első futtatásukkor a programok egyszerűen felvehetők a listára és gond nélkül alkotható hozzájuk szabály.

30 napos kipróbálás után 30 dollárt kell fizetni a Personal Firewallért.

További infók: deerfield.com

Kerio Personal Firewall 2

A program a *Tiny Personal Firewall 2.x utódja*. A *Kerio Personal Firewall* freeware, és tisztán csak a tűzfalfunkciókra korlátozott. Víruskeresőt vagy tartalomellenőrzőt hiába is keresünk benne.



A párbeszédablak részletes információt mutat valamennyi nyitott kapcsolatról

A konfigurációhoz több biztonsági funkciót is kínál, amelyekhez a felhasználó szabályokat definiálhat. A biztonsági fokozat szintjét attól függően kell feljebb vagy lejjebb srófolni, hogy egy megbízható hálózaton vagy az interneten mozgunk-e. A szabályok definiálásánál a Kerio tűzfal rugalmas: lehetőség van a portok, a megbízható hostok, valamint a bejövő vagy kimenő kapcsolatok kiválasztására.

Amikor elindítunk egy internetes programot, például az Internet Explorert, akkor a Kerio Personal Firewall rákérdez, hogy engedje-e vagy tiltsa-e meg a kapcsolatot, és ennek megfelelően maga fogalmaz meg egy szabályt. Ezeken a felhasználó kézzel még változtathat.

A Kerio a biztonság tekintetében *a középmezőnyben* helyezkedik el. A tűzfal valamennyi portot *stealth* állapotba hozza, felismeri a módosított levelező-programot. A Kerio az egyik legolcsóbb megoldás a számítógép védelmére, s némi hálózati ismeretet feltételezve, könnyen lehet a speciális igényekhez alakítani.

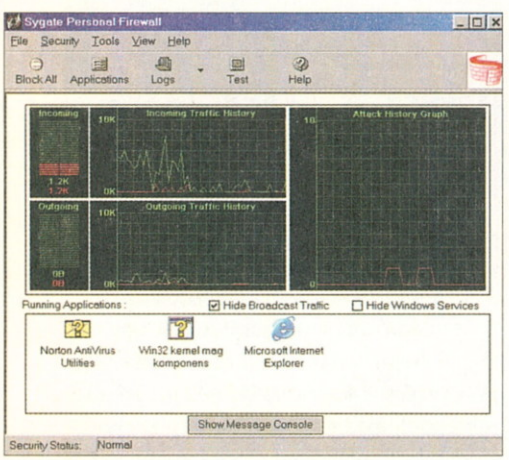
További infók: www.kerio.com

Sygate Personal Firewall 5.0

Hasonlóan a többi személyi tűzfalhoz, telepítése után azonnali védelmet nyújt. A programablakban grafikus állapotjelzők mutatják a hálózati forgalmat és a behatolási kísérleteket. A menük jól szervezettek, gyorsan megtalálhatók bennük a szolgáltatások. A tálcán lévő ikon jobbgombos menüjében ugyancsak elérhetők a legfontosabb lehetőségek.

Háromféle biztonsági szintet kínál az otthoni használatra ingyenes *Sygate Personal Firewall:* a teljes blokkolást, a mindennemű forgalom átengedését és a normál üzemmódot. Amikor egy program először használja az internetet, felkerül az alkalmazások listájára. Itt aztán számos körülményre kiterjedő szabályt alkothatunk arra vonatkozólag, hogy mit tehet meg a későbbiekben. Így például ütemezhetjük futását, vagy korlátozhatjuk használatát bizonyos IP-címekre.

Az eszköztáron található *Test* gomb a *Sygate* webhelyének tesztoldalára röpít minket, ahol gépünk minden lehetséges portját vizsgáló, több órán keresztül tartó próbáknak vethetjük alá védelmi rendszerünket.



Naplózásban verhetetlen a Sygate Personal Firewall

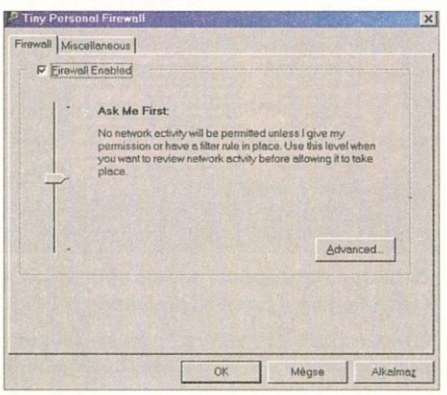
A program naplózási szolgáltatásai egyedülállóak. Részletesen regisztrálja a behatolási kísérleteket, az adatforgalmat és a konfiguráció változásait. Az adatokat többféle bontásban jeleníthetjük meg: az utolsó egy, két vagy három nap, az utolsó egy vagy két hét, vagy pedig az eltelt hónap szerint.

A konfiguráló párbeszédablak jól áttekinthető, bosszantó viszont, hogy egyes szolgáltatások érvénytelenítve vannak, ezeket csak a 40 dollárért megvásárolható *Pro* változatban használhatjuk. A legtöbb felhasználónak azonban nincs is szüksége ezekre, és az 4,6 Mbájtos letöltési méretű ingyenes verzió.

Internetcím: www.sygate.com

Tiny Personal Firewall 2.0.15

A *WinRoute Pro* biztonsági technológiára épülő program felhasználói felülete ennél egyszerűbb már nem is lehetne. Az adminisztrációs ablakot a tálcán lévő ikonra való kettős kattintással jeleníthetjük meg. Három biztonsági szint közül választhatunk, ezek: a teljes blokkolás, az engedélykérés minden adatmozgáshoz és az engedélykérés nélküli működés. Az utolsó esetben minden olyan hálózati aktivitás engedélyezett, amely nem ütközik az általunk korábban meghatározott szabályokba. Akár összetett szabályokat is egyszerűen hozhatunk létre egy világos felépítésű párbeszédablakban. Lehetőségünk van például arra, hogy visszautasítsuk egy adott IP-címről érkező kéréseket. Az adminisztrációs ablak használatát és a naplóállomány megtekintését jelszavas védelemmel láthatjuk el.



Tiny Personal Firewall: puritán felület, hatékony védelem

Amikor nem engedélyezett adatmozgást észlel, a *Tiny Personal Firewall* egy riasztásablakot jelenít meg. Itt engedélyezhetjük vagy visszautasíthatjuk a műveletet, illetve definiálhatunk hozzá egy szabályt, amely meghatározza, hogy miként viselkedjen a jövőben a szóban forgó program.

Az élő kapcsolatok nyomon követésére szolgál az állapotablak, amelyet úgy hívhatunk elő, hogy a jobb egérgombbal a program ikonjára kattintunk, majd a menüben a *Firewall Status Window* lehetőséget választjuk.

Ami a biztonságot illeti, az 1,4 Mbájtos Tiny Personal Firewall szivárgásmentes védelmet nyújt mindkét irányban. Otthoni felhasználók számára ingyenes.

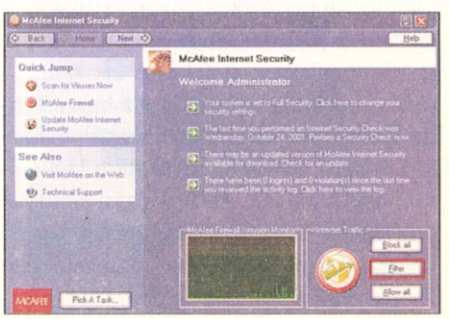
Internetcím: www.tinysoftware.com

McAfee Internet Security

A *McAfee* egy *teljes biztonsági csomagot* állított össze az *Internet Security-vel.* A tartalomszűrővel is felruházott tűzfalon kívül tartalmazza a McAfee víruskeresőt és egy fájl-shreddert is. A program valamennyi telepítési lépésen végigvezeti a felhasználót, és a PC biztonsági ellenőrzését is elvégzi. Eközben cookie-kat és web-bugokat keres a merevlemezen, meghatározza az internetes programokat, és még arról is felvilágosítást nyújt, hogy hol tárolódnak a magánadatok.

Valamennyi internetes kapcsolatot kérő programot egy listában kezel. A felhasználó minden bejegyzésről külön eldöntheti, hogy szabad-e adatot cserélnie az adott szoftvernek, és ha igen, mely porton keresztül teheti ezt.

Kissé el vannak rejtve az olyan beállítások, mint a DHCP és ICMP – ezekhez a felhasználónak egy külön menübe kell belépnie, amely a rendszer hálózati adaptereit tartalmazza. A beállítási sajnos lehetőségek meglehetősen soványkák: az ICMP-t például csak ki vagy be lehet kapcsolni.



A McAfee komplett csomagot kínál

A McAfee program leginkább kritizálható részei a hiányzó beállítási lehetőségek és a szokatlan kezelői felület.

A funkciókat több modulban szétosztották (*Internet Security, Firewall, VirusScan*), ráadásul egyeseket olyan almenükben kell megkeresni, amelyek a *Taszk futtatása* kapcsoló mögött húzódnak.

További infók: www.mcafee.com

Sphinx Personal Firewall

A svájci *Biodata* cég *Sphinx Personal Firewall* programja kettős tagolású. A főablakban egyszer kezdőknek, egyszer

A Sphinx fehér és fekete listákra osztja szét a hostokat

szakértőknek is le lehet hívni a beállításokat. A kezdők beállítását a szakértői beállítás is tartalmazza, csak épp a „szakértő" még további lehetőségeket is kap. A konfigurálást varázslóval végezhetjük. A varázsló nyolc kérdést tesz fel a PC használatával kapcsolatban, például hogy használunk-e webet, e-mail-t, ICQ-t, és hogy vannak-e megosztásaink. A varázsló végül megjeleníti az adatok összesítését.

A Sphinx jellegzetessége *a fehér és a fekete lista*. A fehér lista a megbízható, ismerős hostokat, a fekete lista ennek megfelelően a letiltottakat tartalmazza. Különbséget tesz web, FTP, news és más szolgáltatások alapján. A *Hozzáadás* kapcsolóval mindegyik listához megadható egy host az URL-jével vagy az IP-címével.

A bővített szűrőszabályok azt definiálják, hogy mely csomagok, milyen irányban léphetik át a tűzfalat. A címzettet, a forrás- és célportot, valamint a használandó protokollt valamennyi szabálynál be kell állítani. A Sphinx a TCP/IP-n kívül elboldogul az LLC, az IPX és a NetBEUI protokollal is. Ezzel ezt a tűzfalat Novell hálózatokban vagy kis hálózatokban (NetBEUI) lehet a LAN felől érkező támadások kivédésére használni.

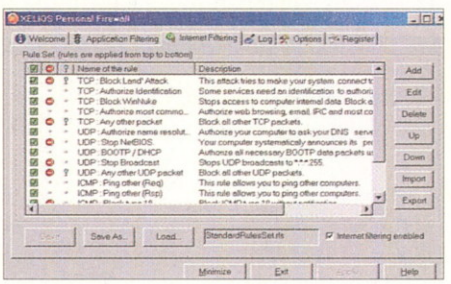
A program trial verziója korlátos: nem lehet eltárolni a konfigurációt.

További infók: www.pcfirewall.com

Xelios Personal Firewall 2.02

A mindössze fél megabájtos letöltési méretű program felhasználói felülete egy többlapos párbeszédablak. A főlapon láthatjuk, hogy milyen IP-címen csatlakozunk az internetre, és folyamatosan figyelemmel kísérhetjük a beérkező és kimenő adatcsomagok számát, illetve azt, hogy ezek közül hányat blokkolt a program. Az *Options* lapon állíthatjuk be a működési jellemzőket, többek között a jelszavas védelmet. Az *Internet Filtering* lapon találjuk az alapértelmezésbeli adatszűrő szabályokat, és itt hozhatunk létre újabbakat.

A biztonsági tesztelés két port esetében *Close* állapotot jelzett, ami azt jelenti, hogy a *Xelios Personal Firewall* megakadályozza az ezeken keresztüli behatolást, a gépünket viszont nem teszi láthatatlanná a külvilág számára. Valószínűleg olyan



Hiába a sok beépített szűrő, nem teljes a Xelios Personal Firewall védelme

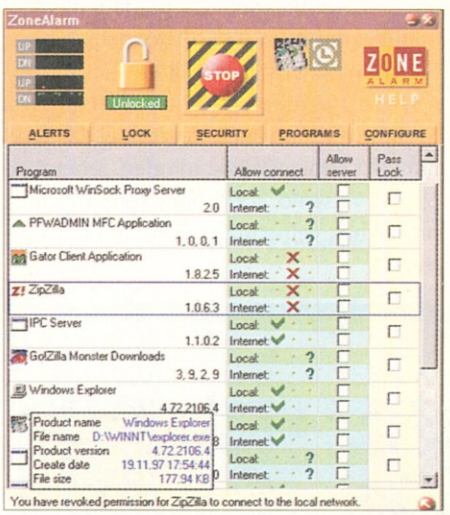
adatszűrő szabály is létrehozható, amely orvosolja a problémát, ez azonban egy személyi tűzfal használójától nem várható el. Ennél is nagyobb hiányossága a programnak, hogy az adatot küldő alkalmazások ellenőrzését csak akkor végzi el, ha bejelöljük az *Application Filtering* ablak *Application Filtering Enabled* lehetőségét. Vagyis amíg erre nem jövünk rá, bármelyik program bármit zavartalanul átküldhet a tűzfalon. Ezután már szigorúan őrködik adataink felett, és a listára felvett programok futási jellemzőit egyszerű egérkattintásokkal módosíthatjuk.

A Xelios Personal Firewallért a 30 napos kipróbálási időszak letelte után 32 dollár regisztrációs díjat kell fizetni. Emiatt, továbbá figyelembe véve hiányosságait, jobban járunk az ingyenes programok valamelyikével.

Internetcím: www.xelios.com

ZoneAlarm Pro 3.0

A *ZoneAlarm*-ot freeware verziója tette ismertté, amely annyiban különbözik a *Pro* verzitótól, hogy nem képes letiltani a reklámokat, valamint a honlap aktív tartalmát. A cookie- és e-mail-mellékletek kontrollja is hiányzik. A Pro verzióban a szabályokat vagy egyes programokra vonatkoztatva, vagy általában határozhatjuk meg. A ZoneAlarm a globális szabályoknál különbséget tesz a *megbízható zónák* és az *internet* között. A felhasználó mindkettőre beállíthatja az engedélyezett portokat és protokollokat.



Egyszerű kezelhetőséggel és tökéletes biztonsággal büszkélkedhet a ZoneAlarm

A tűzfal alapkonfigurálásánál egy varázsló segít. Ha a felhasználónak egy vészjelzéssel kapcsolatban kérdései merülnek fel, akkor a ZoneAlarm összeköti a *Zonelabs* honlapjával, ahol további súgószövegeket talál.

A ZoneAlarm nagy biztonságot kínál, ennek ellenére a konfigurálása nem állítja nehéz feladat elé a felhasználót.

További infók: www.zonelabs.com

Falbontási technikák

A hackerek már régóta próbálkoznak a tűzfalak megfúrásával. Írásunkban bemutatjuk az általuk kifejlesztett eljárásokat és a védekezési lehetőségekről is ejtünk pár szót.

A PC-nk egy tűzfal alkalmazásával még nem válik biztonságossá (ami persze egyáltalán nem jelenti azt, hogy a tűzfal felesleges lenne). Ennek két oka is van. Az egyik, hogy a tűzfal csak bizonyos veszélyek ellen képes védelmet nyújtani, a másik pedig, hogy a tűzfal is kicselezhető. Lássuk, hogy miben áll az egyes programok gyengéje, és hogy hogyan tehetjük ennek ellenére biztonságossá a PC-nket.

Váratlan veszélyek

A tűzfal képtelen védelmet nyújtani a fájlok tartalmából eredő veszélyek ellen. Ilyenek például a vírussal fertőzött adatállományok, amelyeket kétes honlapokról töltünk le. A tűzfal ugyanis nem törődik a vírusokkal, csak azt figyeli, hogy megfelel-e a másik számítógéppel fennálló összeköttetés az általunk megadott biztonsági előírásoknak. Azt, hogy az így fennálló kapcsolaton keresztül érkező adatok veszélyesek-e, a tűzfal nem képes ellenőrizni. Ehhez *külön víruskeresőt* kell telepíteni.

Ma már számos gyártó kínál tűzfalból és víruskeresőből álló csomagokat. Ez a kombináció már jóval biztonságosabbá teszi a PC-t, és feltétlenül javasolható is. Ha netán egy trójainak sikerül is kikerülnie a tűzfalunkat, akkor a víruskereső még mindig megtalálhatja a merevlemezen. A tűzfal másfelől ki is egészíti a víruskereső programot. A víruskeresők ugyanis nem jeleznek a reklám-trójaiak esetén, mert ezeket nem ítélik veszélyesnek. A tűzfal viszont már akkor fedezi fel az ilyen programokat, amikor ezek az interneten keresztül próbálnak kapcsolatot létesíteni.

A tűzfalak a betárcsázó programokkal szemben sem védenek, hiszen csak azt ellenőrzik, hogy mi történik egy fennálló átviteli vonalon, például egy telefonos kapcsolaton keresztül. Ha egy betárcsázó egy új kapcsolati vonalat épít fel, azzal a tűzfal nem törődik, csak az új kapcsolaton keresztül szállított adatokat látja.

A rendszer árulói

A tűzfal az alkalmazásokban vagy az operációs rendszerben jelentkező hibák ellen sem véd. Ha például azt közöljük a tűzfallal, hogy az Internet Explorernek szabad internetes hozzáférést kívánunk adni, akkor egy hacker felhasználhatja ezt a programot arra, hogy kárt tegyen a számítógépünkben. Ez a programhibák (az exploitok) kihasználásával történik. A hibák megszüntetéséért a gyártók többé-kevésbé rendszeresen patcheket jelentetnek meg, amelyekkel célszerű aktuális szinten tartani az operációs rendszerünket és a szoftvereinket.

Hogyan védekezzünk?

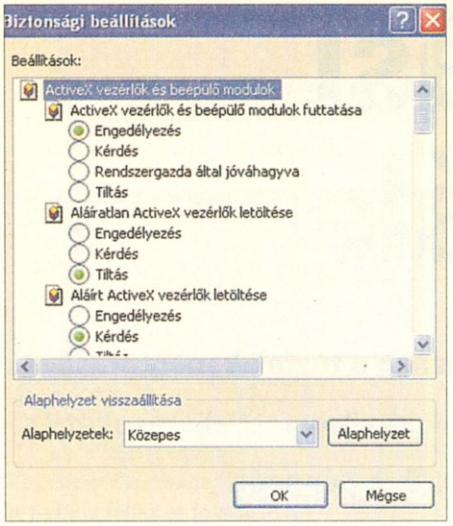
Az amerikai *Edelman* ügynökség nemrég nyilvánosságra hozott felmérése szerint csaknem minden harmadik gép hacker- vagy vírustámadás áldozatává válik, nem kis veszteséget okozva ezzel a cégeknek és a magánszemélyeknek. Két hazai szakértőt kértünk meg a hatékony védekezés bemutatására.

A hackerek aktivitásának és a vírusok terjedésének helyzete hazánkban is hasonló, azonban még mindig kevesen gondolnak a hatékony védekezésre. Pedig a „miért pont velem történne meg" szemlélet létjogosultsága már számtalanszor megdőlt. A tűzfalak – akár hardver-, akár szoftveralapúak –, szinte kivétel nélkül alkalmasak a számítógépes betörések megakadályozására, vagy legalább megnehezítésére – mondja *Imre Balázs*, a *Telindus Hungary Kft.* tanácsadója. A tűzfal minden információcsomagot értelmez, és eldönti, hogy az keresztül mehet-e rajta avagy sem – magyarázza *Kiss Szabolcs*, a *Symantec Magyarország Kft.* rendszermérnöke.

A hardveralapú védelem előnye, hogy nem kell telepíteni. A működtető rendszer erőforrásai úgy vannak összeállítva, hogy azok a legjobb teljesítményt nyújtsák. Az eszköz általában kisebb méretű, az általános hardvereknél könnyebben elhelyezhető. Nem szükséges hozzájuk monitor, billentyűzet stb. A kezdeti költségek viszont nem túl alacsonyak, így az alkalmazását inkább a közepes és nagyobb cégeknek, vállalatoknak ajánlja Imre Balázs.

A szoftveres tűzfalak előnye az alacsonyabb induló költség, és az, hogy nem szükséges külön menedzsment gépet üzemeltetni. Kisebb viszont a teljesítményük, azaz nagyobb mértékben lassítják a rendszereket, mint a hardveralapúak. A használathoz a programot telepíteni kell, és ha igény van a teljesítmény növelésére, a működtető hardvert kell nagyobb kapacitásúra cserélni – fűzi hozzá Kiss Szabolcs.

Az viszont biztos, hogy mindkét védekezési forma hatékonyan óv a hackerek támadásaitól és igényeink, illetve pénztárcánk szerint széles skálában választható megfelelő megoldás a magyar piacon – teszik hozzá a szakemberek.



Célszerű letiltani az ActiveX elemeket

Persze a hackerek nemcsak a programhibákon keresztül képesek kárt okozni, a szabályos programfunkciókkal is képesek visszaélni. Különösen veszélyesek az *ActiveX vezérlők,* amelyeket az Internet Explorer vezérel. A legjobb, ha az *Eszközök/Internetbeállítások* menüben a *Biztonság* regiszterlapon kikapcsoljuk ezeket. Az *Egyéni szint* kapcsolóval megjelenő listában célszerű az összes ActiveX objektumot letiltani. Ez viszont a plugineket, például a Flash Playert is érinti.

Az egyik sandbox rendszer: a surfin Gate

Ezért érdemes minden szörfözés előtt eldönteni, hogy mekkora biztonságra és mennyi böngészőfunkcióra lesz szükségünk. Minthogy a scriptek is veszélyesek, az előbb említett biztonsági opció listában az ActiveX vezérlők és a beépülő modulok opciót is le kell tiltani, vagy legalábbis *Kérdés* feltételre kell korlátozni. Ha egy tűzfalnak nincsen tartalomszűrése, akkor hatástalan a scriptekkel és a Java modulokkal szemben.

Az exploitok és a túl nagy teljesítményű alkalmazások ellen a *sandbox rendszerek* nyújthatnak segítséget, például a *Surfin Gate* a *Finjan-tól* (**www.finjan.com**). Az ilyen rendszerek korlátozzák a programok tevékenységét: a felhasználó maga adja meg, hogy mit akar megengedni az egyes programoknak. Ha ezután egy exploittal valami mást szeretne végeztetni, akkor az akció a sandboxon elakad, feltéve persze, hogy a sandbox működik, különben a PC-kre érvényes egyéb biztonsági előírások érvényesek. Ha egy webszerver elérését engedélyezzük, akkor ezt egy hatékony jelszóval (minimum nyolc karakter, lexikonban fellelhető fogalmakat ne használjunk) kell védeni. A tűzfal képtelen megvédeni az olyan hackertől, aki látszólag legálisan, feltört jelszóval jelentkezik be a szerverünkre.

Vékony falak

Egyetlen szoftver sem teljesen hibamentes, és ez a tűzfalakra is érvényes. Éppen ezért a hackerek is mindig találnak újabb exploitokat, amelyekkel kicselezhetők vagy lefagyaszthatók a tűzfalak. Ez részben olyan programokkal működhet, amelyek célirányosan képesek adatcsomagokat létrehozni.

Az internet TCP/IP protokolljával küldött valamennyi adat csomagokra bontódik. Ezek a csomagok a tényleges adatokon kívül a feladóról és a címzettről is tartalmaznak információkat. Ennek az információnak adott formátumúnak kell lennie, hogy olvasni lehessen. Speciális segédeszközökkel egy támadó „hibás" csomagokat hozhat létre, amelyek nem felelnek meg a protokollban előírt formátumnak, vagy ellentmondásos adatokat tartalmaznak. Az ilyen hibás csomagot kapott alkalmazásnál ez „cigányútra futhat", vagyis az alkalmazás lefagyhat.

A tűzfalnak voltaképpen fel kellene tartóztatnia az ilyen csomagokat, de az is megeshet, hogy maga a tűzfal is lefagy tőle. A legrosszabb esetben a számítógépünk védtelenné válik. Veszélytelen esetben a teljes rendszer lefagy, és a PC egy ideig elérhetetlen, még a hacker számára is. Az ilyen veszélyektől csak a rendszeres update-ek óvhatnak meg bennünket.

Bizonyos tűzfalak internet felőli átfúrására szolgál az *IP-Spoofing* módszer. Ez érinti az összes olyan szolgáltatást, amely IP-címeket használ a *megbízhatónak* minősített számítógépek beazonosításához. Megbízhatónak számítanak a saját hálózat munkaállomásai és szerverei, de a cég internetszervere is, amelyről az e-mailjeinket vagy az update-jeinket kapjuk.

Ha rendelkezünk egy olyan segédprogrammal, mint amilyen a Linux *Nemesis-e,* amellyel tetszőleges adatcsomagok hozhatók létre, akkor ezzel meg lehet hamisítani az adatcsomagok feladójának a címét, s a hacker így hamis identitást mímelhet. Ha a megtévesztés sikeres, akkor a támadó adatcsomagokat tud a tűzfalon átjuttatni, vagy akár egy futó hálózati kapcsolatba is képes beilleszkedni.

Az IP-Spoofing mindenekelőtt olyan tűzfalakat érint, amelyek az adatcsomagok szűrésén kívül nem sokat kínálnak, és nem tudják megkülönböztetni a LAN vagy az internet felől érkező csomagokat.

Így védhetjük meg a PC-nket

Az alábbi öt tipp kellő védelmet nyújt a felhasználónak:

1. Telepítsünk egy tűzfalprogramot.

2. Mindig a tűzfal és a böngésző szoftver legújabb verzióját használjuk. Rendszeresen keressük meg a legújabb update-eket és patch-eket.

3. Ne használjunk olyan programokat, amelyek lényegesen több funkcióval rendelkeznek a számunkra szükségesnél. Valóban programozhatónak kell lennie a levelezőnknek? Tényleg olyan mélyen be kell nyúlnia a böngészőnknek az operációs rendszerbe, mint azt az Internet Explorer teszi az ActiveX vezérlőkkel? Valóban hozzá kell egy chat-elő programnak férnie a fájlrendszerhez, mint az ICQ-nál? Minél kevesebbet tud egy szoftver, annál kisebb a valószínűsége annak, hogy nagy károk keletkezhetnek egy exploittal. Kétséges esetben használjunk nyílt forráskódú programokat. Biztosak lehetünk abban, hogy nem tartalmaznak olyan rejtett funkciókat, amelyektől a tűzfalunk nem képes megvédeni. Ezen kívül az ilyen programok hibáit hamarabb fedezi fel és szünteti meg a programozók közössége.

4. Használjunk aktuális aláírással rendelkező víruskeresőt, és rendszeresen szkenneltessük végig a PC-nket.

5. Ne nyissunk meg gyanús mellékleteket, és csak megbízható forrásból származó programokat telepítsünk. Ha ugyanis trójai program vagy más hackertool jutott be a gépünkre, akkor adott esetben egy tűzfal sem tud segíteni.

Kislexikon

Exploit: Olyan módszer, amellyel a támadó képes kihasználni az ellenfele szoftverhibáit vagy PC-jének biztonsági hiányosságait.

IP-cím: Egyfajta „telefonszám", amellyel a hálókártyánk egy TCP/IP alapú hálózatban rendelkezik. Az ilyen címek formátuma 255.255.255.255, vagyis például 127.0.0.1.

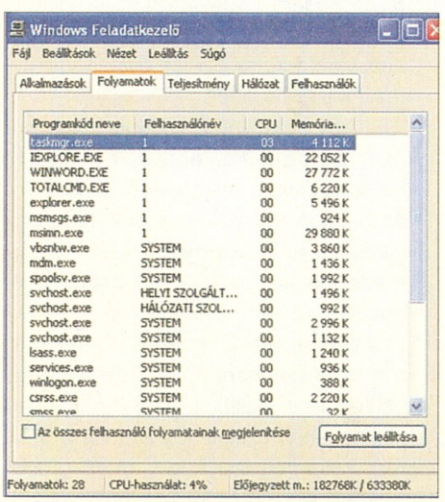
Trójai program: A saját PC-nken garázdálkodó program, amely az internetről érkező támadás támpontjaként és hídfőjeként képes működni. Ha létrejön az áldozat gépen egy ilyen hídfő, akkor a gépe távvezérelhetővé válik. A felhasználó összes billentyű- és egérművelete a támadó számára láthatóvá válik. A trójai programok, a vírusokhoz hasonlóan, fertőzött állományokkal terjednek.

Reklám-trójai: Olyan program, amely egy adott gyártóval hoz létre kapcsolatot. Ezek a programok néhány kommersz programmal, de ingyenes szoftverrel is hozzánk kerülhetnek. A céljuk marketing jellegű, de nemcsak reklámot, hanem a felhasználóval kapcsolatos adatokat is képesek továbbítani.

A szennyezett PC

A tűzfal félig már meg is van törve, ha a támadónak sikerült az áldozata gépére telepíteni egy trójait vagy általánosan egy RAT-et (*Remote Access Tool*).

A tűzfal megkerülésének a legegyszerűbb módszere a tűzfal leállítása úgy, ahogy a Windows *Feladatütemező* a **Ctrl+Alt+Del** billentyűkkel leállít egy programot. Ehhez a támadónak azt sem kell tudnia, hogy melyik tűzfal fut, csupán egy olyan programot kell írnia, amely becsukja az összes ismert tűzfal eljárást. Ez az eljárás azonban feltűnő, mert a felhasználó észreveheti a tálcáról hiányzó ikont.



Ez is egy megoldás: „Ctrl+Alt+Del"

Egy másik módszer a tűzfal működési módszerének az ismeretét feltételezi. A tűzfalak a nevükről ismerik fel az internethez engedhető programokat. Ezt a védelmet egy támadó könnyen kicselezheti. A hacker például *iexplore.exe-nek* kereszteli el a programját, és máris az összes, az Internet Explorernek adott joggal rendelkezni fog. Az aktuális tűzfalak egy ellenőrző összeg segítségével azonosítják az igazi Internet Explorert. Ha az eredeti exe fájl módosul vagy egy hamis fájl jelenik meg, akkor a tűzfal vészjelet küld.

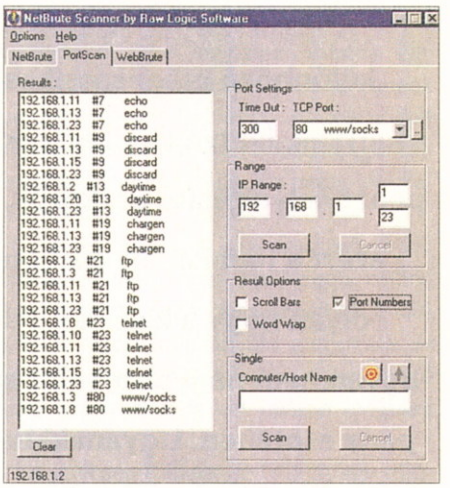
A *Tooleaky* segédprogram más utat követ. Titokban megnyitja az Internet Explorert, betölt egy internetlapot és erről a lapról tartalmat tölt át az áldozata gépére. Mivel a legtöbb felhasználó az Internet Explorert használja böngészésre, így a tűzfal megengedi az Explorernek a lapok letöltését, anélkül, hogy előbb figyelmeztetné a felhasználót.

Egy másik eljárás még ennél is tovább megy. A trójai program meghívja az Internet Explorert, majd a saját kódját hozzátoldja ahhoz a tárterülethez, ahol a böngésző fut. Tehát nem a merevlemezen lévő fájlt módosítja, hanem a RAM-ba töltött kódra akaszkodik. A tűzfalnak úgy tűnik, mintha az Internet Explorer tevékenykedne, ténylegesen viszont a trójai program fér hozzá az internethez.

Hamis portok

Ha egy tűzfal nem követi, hogy mely programok mennek ki az internetre, akkor újabb kerülőutakat tesz lehetővé. Példák erre az *alagútprogramok*. Minden internetkapcsolathoz egy port van hozzárendelve, a HTTP-hez (Hypertext Transfer Protocol) például a port 80. A portszámok egy társasház névtábláihoz hasonlíthatók. A háznak – vagyis a hálókártyának – egy saját IP-címe van. Az operációs rendszer a portszámból tudja, hogy a ház melyik felhasználói programjához tartoznak a bejövő adatok.

Speciális programokkal egy „hamis" porton is át lehet küldeni az adatokat, tehát a port 80-on egy Telnet-es kapcsolatot is lehet létesíteni. Ez egy hacker számára akkor célszerű, ha a 23-as Telnet-port le van tiltva. Ekkor a Telnet-adatok a HTTP csomagok közé kerülnek. A feltétel csak annyi, hogy az ellenállomás ismét ki tudja csomagolni a becsomagolt adatokat. Ezt az eljárást *tunneling-nek* nevezik.



Portokból nincs hiány – de vajon, melyik van nyitva?

Bizonyos programok, mint például a *Leapfrog*, az egyik portról egy másikra irányítja át az adatokat. A 80-as portra beérkező adatok a 23-as portra továbbítódnak, s így lehet Telnet-es kapcsolatot létesíteni, holott csak a 80-as port van nyitva.

Rizikó analízis

Zonealarm – az egyik legnépszerűbb „personal" tűzfal

Talán a fenti példákból is világossá vált, hogy egy tűzfal nem jelent semmilyen biztonsági garanciát. Pánikra azért nincs ok, mert ha nem üzemeltetünk webszervert és nincs nagysebességű állandó vonalunk sem, akkor egy hacker számára érdektelenek vagyunk. Ebben az esetben egy tűzfal, egy víruskereső és némi szakmai hozzáértés is elég a biztonság megőrzéséhez. ■

Kártyajátékok

A hitelkártyák és a különböző mágnescsíkos kártyák, illetve chipkártyák pénzt helyettesítő eszközök, ezért a hamisításukra épp olyan nagy a kísértés, ha ugyan nem nagyobb, mint a pénz esetében. Ugyanakkor azt is el kell ismernünk, hogy a legtöbb kártya hamisítása nem igazán nehéz feladat. A bankok Magyarországon is számolnak a kártyacsalás kockázatával, együttműködésük következtében azonban ez a kockázat még elviselhető.

Érdemes megnézni azokat a módszereket, amelyekkel megkopasztható az ügyfél és a bankja, hogy amennyire csak lehetséges, védekezni tudjunk ellenük. A legfontosabb: van néhány aranyszabály, amelyet be kell tartanunk, ha plasztikkártyát használunk, ezek egyben a mindennapi túlélés szabályai is.

A kártyahasználat szabályai

1. Soha ne írjuk fel a kártya titkos azonosító kódját. A PIN-t telefonon se mondjuk be soha, a bank ilyet nem kér, legfeljebb a nevében bejelentkező csalók. Ha a bank nevében kérik a kódot, az mindenképpen beugratás. A banki telefonos tranzakciók során más PIN kódot használunk, amelyet a bankkal való megállapodásunk rögzít. A bankok megint más kódot alkalmaznak az internetes home banking szolgáltatásaikhoz.

2. A PIN kódot, ha a bank rendszere engedi, a kézhezvétel után azonnal változtassuk meg olyanra, amelyet könnyen meg tudunk jegyezni. A legtöbb bank ezt ingyen vagy minimális díjért megengedi. Ezzel elkerüljük a PIN felírásának biztonságot alaposan rontó műveletét. Ha megváltoztattuk a PIN kódot, akkor nyugodtan a kártya mellett hagyhatjuk az eredeti – immár nem érvényes – cetlit a PIN kóddal. Ezzel elősegítjük, hogy néhány rossz próbálkozás után az automata elnyelje a kártyát.

3. A tranzakciókról kapott nyugtát sohase hagyjuk a helyszínen. A rajta szereplő adatokkal visszaélhetnek! A legtöbb esetben rajta van a teljes kártyaszám vagy annak nagy része, amellyel például visszaélhetnek az interneten. Jobbfajta banki automatáknál kérhető, hogy ne adjon bizonylatot. Vásárláskor ez sajnos kötelező.

4. Amennyiben lehetséges, kérjünk a tranzakciókról rádiótelefonos automatikus értesítést, így idejében fel tudjuk fedni a klónozásos csalásokat .

5. A kártyalehúzáskor ne engedjük, hogy elvigyék a kártyát a szemünk elől. Kísérjük végig a kártya útját, mert ezzel meg tudjuk akadályozni a másolatok készítését.

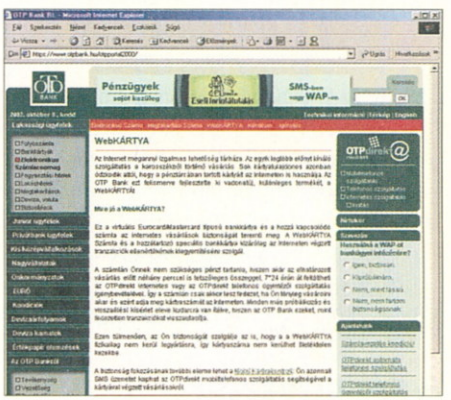
6. A hó végi kimutatásokat és a bizonylatokat vessük össze. Ezzel felfedezhető a duplázásos csalások nagy része.

7. Több kártyánk legyen, különböző pénzintézeteknél. Mindig azt használjuk, amelyik hitel- és limitfeltételei a vásárláskor a legoptimálisabbak. Ezzel elkerülhetjük, hogy pénz nélkül maradjunk. Ezeket a kártyákat sohase tartsuk egyetlen helyen.

8. Bármilyen visszaélés gyanúja esetén tiltsuk le a kártyát. Ezzel a klónok is használhatatlanná válnak! Olcsóbb kifizetni a tiltást, mint futni a számlánkon tartott pénz után.

Ennyi jó tanács után nézzük, miféle furfangokkal tudják kifosztani az ügyeskedők a pénztárcánkat és a bankot egyaránt. Ehhez tudnunk kell, hogy a kártyahasználat során kétféle fizetési módszert alkalmazunk.

Az egyik a *card present* típusú fizetés, ahol a kártya fizikailag is jelen van a fizetés során. A kártyák egy részén erre szolgál a *CV kód* is az aláírássávon. A másik a *card not present* típusú fizetés. Ilyenkor a kártya nincsen jelen, a kártyaadatok megadásával kezdeményezünk fizetést. Az ilyen típusú fizetésekkel követik el a visz-



A virtuális bankkártya: az OTP webkártyája

Hitelkártya-generátorok: beszélgetés

JoY, a hitelkártya-generálás nagy szakértője: a saját elmondása szerint eddig nagyjából 80 ezer dollár értékben használta mások hitelkártya-számait. Saját magáról csak annyit árult el, hogy külföldön él, de magyar származású – beszélgetésre szigorúan csak ICQ-n keresztül volt hajlandó.

– Az első és legfontosabb szabály: a generált kártyaszámot semmiképpen se árucikkek rendelésére használd, azaz ne vásárolj vele. Hogy miért? Hát logikus – mert ahhoz meg kell adnod a címedet, legalábbis ha kell a cucc. Egyenes út a sittre...

– Ez ennyire büntetendő dolog?

– Hah! De mennyire! Olyan mint egy bankrablás kicsiben. Ha jó hacker akarsz lenni, akkor először is a problémát kell megvizsgálnod, majd megismerned. Csak azután kezdhetsz neki a

Az OTP többféle bankkártyát kínál ügyfeleinek

szaélések nagy részét. Most pedig tekintsük át a kártyahamisítások legfőbb fajtáit.

Kamulálás

A módszer lényege, hogy egy nem létező, de hihető kártya adatait hozzuk létre. A számítástechnika alvilágában megtalálható számtalan programcsomag segítségével minden további nélkül létrehozhatunk ilyen kártyaszámokat, mégpedig vagy a saját kártyaszámunk extrapolálásával vagy pedig teljesen új számok generálásával.

A kártyaszám felépítése teljesen publikus. Az első számcsoport adja a kártyafajtát és a bankot, a következők a típus- és a sorszámot, amelyeket a végén egy ellenőrzőszám követ. Egyes kártyatípusoknál létezik még egy card present ellenőrzőkód is a kártya hátoldalán, amely a kártyaszámot követi, de ennek itt nincs jelentősége.

Az InterCard POS terminálja analóg vagy ISDN vonalon egyaránt működtethető

Ha ezeket a generált számokat és a melléjük költött, de hihető adatokat a neten kisösszegű fizetésekhez használják fel – általában 5 dollár vagy 10 német márka alatt – akkor a rendszer csak negatív lista alapján végzi el az autorizálást, azaz azt nézi, szerepel-e a kártya a letiltottak között. A meglopott cég csak akkor kap észbe, amikor a banktól le akarja hívni az összeget.

A bankok ilyenkor általában fizetnek, a kisösszegű kár jelenleg éppen a kezelhető kockázat körébe tartozik. Lebukás esetén viszont a „díja" ugyanaz, mintha egy ezerforintost hamisítottunk volna. Vannak ugyanis olyan, bankkal összefonódott szervezetek is, amelyek a kisösszegű kifizetéseket is autorizálják. Ez pedig lebukási kockázattal jár.

Ha az adatokat mágnescsíkra írják, egy-két helyen még kisösszegű online tranzakciót is kezdeményezhetnek a kártyával, hiszen a társbanki autorizálás is pénzbe kerül, és a bankok a kezelhető kockázat mértékéig ezt inkább magukra vállalják.

A jelenség tömegessé válását egy idióta – de ma is egyre gyakrabban alkalmazott – amerikai jogszabály idézte elő, amelynek nyomán az internetes szexoldalak, mégha ingyenesek is, hitelkártyaszámot kérnek a nagykorúság igazolására, egyes szolgáltatók pedig szolgáltatásaik ingyenes kipróbálását is hitelkártyaszám megadásához kötik. Ez az egyetlen eset, amikor a saját érdekünkben kamulált kártyaszámot kell használni. Ezek a rendszerek – ellenőrizhetetlenségük, adatkezelésük miatt – a kártyaszám-lenyúlások leggyakoribb forrásai. Vagy pedig ne nézzük a széplányokat ilyen helyeken!

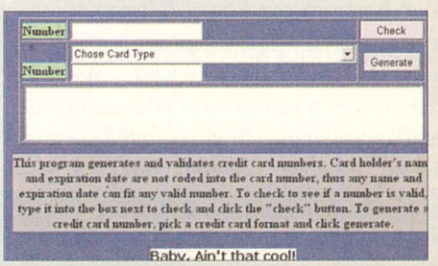
A tanulság egyértelmű: a plasztiklap fizetésre való és nem másra. Aki másra használja, az jogosulatlan adatkezelést követ el, és elősegíti a hamisítási üzletág felvirágzását. A kamulálás esetében a

JoY-jal.

megoldásnak, ha a problémát már úgy ismered, mint a tenyeredet. Szóval, először is megnézed a problémát – azaz magát a számot. Előveszed szépen a zsebedből a kártyácskádat és megvizsgálod. Mondjuk VISA kártyád van. Azt látod, hogy van 4 szám, majd kötőjel, aztán megint 4 szám és így tovább. Azaz: 4-4-4-4. A legáltalánosabb a 4-3-3-3 és a 4-4-4-4 variáció. Persze többféle verzió is van, nálunk például spéci kártyák is léteznek (4-4-4-3), de most csak a legáltalánosabbakat nézzük. Szóval van négyszer-négy szám. Nézzük alaposabban! Kis utánaolvasással (több kártya megvizsgálásával) és némi logikával érthetővé válik a dolog: az első számjegy a kártya típusát írja le – ez a típusazonosító. Ha az első szám 4-es, akkor az VISA Electron, ha 5-ös Mastercard, és így tovább. Az azonosító utáni három szám a számlavezető bankot azonosítja – ha megnézel két kártyát, ami ugyanabból a bankból van, erre is könnyen rájöhetsz. Ezzel a négyszer-négy számból az első négy meg is van. A következő négy szám már húzósabb – ezt a bank rendszere alakítja ki minden ügyfélnek külön, mégpedig úgy, hogy a számla kredit-határát és a lejárati időt kiszámolja egy képlet alapján. A lényeg, hogy a hitelkártya számok a Luhn-féle ellenőrzőösszeg-képzés alapján megvizsgálhatók – ez egyszerű matematika. Nézzük: egy érvényes, 4-4-4-4 kártya számaiból a ***** képlet alapján a végső összeg osztható 10-zel. Na most, ha a végső összeg osztható 10-zel, akkor az egy érvényes hitelkártya-szám. Mondanom sem kell, hogy ez visszafelé is működik.

– *Akkor már meg is van a szám?*

– Hát az még nincsen meg – úgy kell generálnod, hogy az azonosító és a bankfiók „rendszáma" létező legyen. Viszont ha



Ilyen egyszerű egy hitelkártya-generátor

kész vagy, még akkor sem biztos, hogy ez egy létező kártya – csak annyit jelent, hogy a szám „mögött" elvileg lehet egy kártya. Itt szükség van egy kis trükközésre, a legegyszerűbb a szextelefon vagy a pornóoldalak – ezek a rendszerek általában nem logolnak meg semmit, szóval csak beütöd a számot és vagy jó, vagy nem. Addig próbálkozol, amíg nem találsz 10-15 létező számot, ezekkel azután elvagy egy pár napig, hétig.

veszteség azt a bankot terheli, amelynek a kártyáját kamulálták, illetve ha nem fizet a bank, akkor a szolgáltatót.

A további csalástípusok már a kártyabirtokos számlájára mennek, éppen ezért a kispénzű emberek számára igencsak veszélyesek. A csalók ügyesek, és általában a számlákat, sőt a hitelkeretet is teljesen lefosztják. Ilyenkor egyetlen lehetőség marad: a bankkal való hosszadalmas egyezkedés, a rendőrségre járás, de még akkor sem lehetünk biztosak abban, hogy hozzájutunk-e a pénzünkhöz, vagy pedig a bank nyilvánít bennünket nem kívánatos személynek. A bankok nem szeretik a problémás ügyfeleket.

„Liftes csalás"

Az internetes kereskedelemben jelent meg a legújabb trükk, amelynek a károsultja a bank és az internetes kereskedőház. Az egyre terjedő módszer szülőatyáit a közelmúltban küldték hűvösre Oroszországban, de a módszert mégis sokan alkalmazzák.

A módszert mindig valamelyik internetes áruházzal szemben vetik be. A csaló ilyenkor bankszámlát nyit, mondjuk Ukrajnában, majd utána honlapot indít a neten. A honlapján egy az egyben hirdeti a kiszemelt internetes áruház kiszemelt termékeit. Fizetni átutalással kell, mondjuk a megadott ukrajnai vagy akár kajmán-szigeteki bankszámlára, esetleg le is tudja hívni a pénzt a hitelkártyáról. Mivel a megrendelés is valahol a világban megbúvó barátunkhoz fut be, ő ilyenkor folytatja a mókát. Máskor a pénzt fogja el, és nem fárad további ténykedéssel, mondjuk az áru vagy a szolgáltatás értékesítésével. Csupáncsak hamis linkeket helyez el a világban, amelyek beterelik hozzá a gyanútlan felhasználót. A vevő adataival, annak nevében immár más áruházakban is megrendeli az árukat és szolgáltatásokat, neki szóló szállítási címmel. Vagy az egész adatbázisát egyszerűen eladja más csalóknak.

A másik módszernél lopott hitelkártyával fizet a jó helyett, amelyről ő inkasszált az eredeti áru hirdetőjénél. Ilyenkor az áru megjön, csak a pénz nem a szolgáltatónál köt ki. Így a csalónak megmarad a teljes összeg tisztán, az áruház, a hitelkártya-társaság és a hitelkártya igazi birtokosa pedig elvitatkozhat az összeg jogosságán. Az amerikai tapasztalatok szerint az árut természetesen nem adják vissza azok, akik megrendelték, hiszen fizettek érte. A szállítási cím, meg a bankszámla közötti távolság senkinek sem tűnik fel, hiszen a jelenlegi adó- és vámrendszerek még sok esetben a nyugati polgárokat is ügyeskedésre kényszerítik.

Teljes körűen felhasználható Eurocard-MasterCard bankkártyát

Az Inter-Európa Bank tiniknek szánt bankkártyája belföldön és külföldön egyaránt használható

A kártya klónozása

A klón annyit jelent, hogy az egy példányban létező kártyát valamiféleképpen megtöbbszörözik, s az eredeti kártya és a klónja az eset felderítéséig egyszerre létezik az időben. És természetesen amíg le nem bukik a számlaegyenlegek egyeztetésével, más is fizet a mi kártyánkkal.

A klónozásnak több alaptípusa ismert.

Ikresítés

Az ikresített kártya *pontosan* azonos az eredetivel. A kártyát ilyenkor még egyszer lehúzzák, majd a lehúzott kép mellé a mágnescsíkot is lemásolják. Utána következik a legnehezebb dolog, a kártya tökéletes másolatának az előállítása. Ehhez általában több lopott, lejárt, de a hamisítandóval megegyező kártyát használnak. A legmacerásabb hamisítás ez, mert ezredmilliméteres pontossággal, darabokból állítják össze az új kártyát, amely a megtévesztésig hasonlít az eredetire. Természetesen a fényképes kártyák erre alkalmatlanok. Az ikresített kártyát pontosan úgy használják, mint az eredetit, és az az előnye is megvan, hogy a hátlapon az aláírást a hamisító kicserélheti a sajátjára. A kártyatársaságok ezért helyeznek el az utóbbi négy-öt évben biztonsági jegyeket az aláírássávon is. A módszert elsősorban a jó kézműves kultúrájú országokban használják, de Törökországban, Olaszországban is előfordul. Előnye, hogy a beváltáshoz nem kell beavatni a kereskedőt is.

Stemplizés

A beavatott szám-összeszedő még egyszer lehúzza a papír slipet a beváltás során. Ez kerül át a kártyahamisítókhoz. Ők ennek alapján a bélyegzőkészítéshez hasonló eljárással elkészítik a kártya dombornyomású részét. Utána ezek a stemplik elkerülnek a beavatott kereskedőkhöz, akik erről hagyományos papírslipesgyalus módszerrel lehúzzák a banki papír slipet, és benyújtják a fizetési igényt. Amikor megjön az általában egyszerre nagyobb tömegben benyújtott levonatokért járó pénz, a vállalkozás eltűnik.

Duplázás

Ekkor a csaló kereskedő vagy legalább kétszer húzza le a papír slipet, majd a második garnitúrát is benyújtja, vagy pedig az elektronikus kártyaolvasó POS-t manipulálják. Ebben az esetben a POS akár a PIN kóddal együtt is tárolhatja a korábbi tranzakciókat, amelyeket újra el lehet küldeni más összeggel. Ez a fajta manipuláció, ha ügyesen csinálják, eléggé nehezen leplezhető le, csak a terhelések pontos nyilvántartása segíthet. Ilyenkor általában viszonylag kis összegekkel és többször próbálkoznak.

A fejlettebb megoldásnál ezek az adatok kinyerhetők a manipulált POS memóriájából, és akár a világ másik pontján is újra felhasználhatók.

Felírás

Magyarországon ez a módszer igen divatos volt egyes helyeken, mára azonban jelentősen visszaszorult. Évekkel ezelőtt az M1 akkor még kapukkal ellátott fizetős szakaszán ilyen típusú visszaéléseket leplezett le a rendőrség. Itt annyi történik, hogy a kártyát még egyszer lehúzzák a hivataloson kívül. Erre egy apró, tenyérben nagyon jól elrejthető eszközt alkalmaznak, amely pár száz mágneskártya mágnescsíkjának tartalmát tudja megőrizni a memóriájában. A felírók általában fejpénzt kapnak a lehúzott kártyák után.

Íme egy tipikus vendéglői POS terminál (a RestaurantPlus cég terméke)

A Fujitsu POS terminálját a gyorséttermekben használják

Az így megszerzett adatok nem tartalmazzák a PIN kódot, ami azt jelenti, hogy áruvásárlás céljára használhatók fel. A világban a bűnszövetkezeteknek számos beavatott partnerük van. Ezek a felírt mágneskártyasávot adatvonalon keresztül megkapják, majd újra kiírják egy akármilyen plasztiklapocskára. A technológia nem bonyolult, alig száz euróból, kereskedelmi eszközökből összerakható. Az ügyfél nevében a hamisítvánnyal olyan kereskedőknél vagy pénztárosoknál vásárolnak, akik nem akarják észrevenni, hogy nem hitelkártyát húznak le hitelkártyakánt. A kapott árut azután újra értékesítik, így jutnak a pénzükhöz.

Kártyaszám-adatbázis lopás

Az internetes kereskedelemben van egy rossz szokás: a cégek adatbázisokban tárolják az ügyfeleik kártyaszámát. Ha ehhez az adatbázishoz valaki hozzáfér, olyan adatsort szerezhet meg, amely az elektronikus kereskedelemben, pontosabban a *card not present* típusú fizetéseknél használható fel.

A dolog még súlyosabb, ha a cégnél nem is a neten lévő, de különben jól védett adatbázist lopja el egy illojális alkalmazott, amire szintén van példa bőven. A leleplezés itt is csak a kártyás tranzakciók követésével lehetséges.

Összefoglalva megállapíthatjuk, hogy a kártyahamisítások és manipulálások köre igen széles. A jó rendszer, a lojális alkalmazottak csak csökkenteni tudják a veszélyt. Ugyanakkor fenyegető az a jelenség is, amelyet itthon lehet tapasztalni, hogy egyes kereskedőhelyek a fizetéskor kérik a PIN kódot, amely így könnyen „lesasolható". A gépek manipulálási lehetőségeitől eltekintve a boltokban nincsenek meg a PIN beadásának korrekt feltételei.

A jövő valamivel nagyobb biztonságot ígér. De ez a biztonsági többlet az életet is megnehezíti. Ilyen például a chipes bankkártya, amelynek használata a leolvasóktól és az ezekkel ellátott számítógépektől függ. A megfelelő intelligens eszközök jó pár primitív trükköt ellehetetlenítenek ugyan, de a *card not present* típusú fizetéseknél továbbra is fennáll a csalás lehetősége. A klónozás nehezebbé válik, de ha a rádiótelefon kártyát is klónozni lehet, akkor semmi sem lehetetlen.

A bankok a hamisítás ellen egy újabb módszerrel is védekeznek. Ez a *felhasználói profil követése*. Azaz igyekeznek kiszűrni az olyan típusú tranzakciókat, amelyek szokatlanok. Ilyenkor – a normálisabb banknál – rövidesen csörög a telefon, és így kérnek megerősítést. A kevésbé normális banknál az ügyfélnek kell kinyomoznia, vajon miért nem működik a kártyája, mondjuk Szingapúrban.

Persze ez a módszer is csak akkor ér valamit, ha jól alkalmazzák. Egyes bankok azonban – orwelli módon – a felhasználói profil követésével próbálnak következtetéseket levonni az ügyfélre – például annak egészségi állapotára – vonatkozóan, hogy megállapítsák, milyen feltételekkel érdemes neki hitelt adni. És erre a kártyánál ideálisabb eszközt keresve sem találni...

K. J.

Nehézbombázók

Bármilyen rosszul is hangzik az elnevezés, a levélbomba vagy „e-mail bomb" nem azt jelenti, hogy a gyanútlan áldozat postai úton dinamitrudakat kap. A levélbomba egész egyszerűen annyit jelent, hogy az áldozat e-mail-címére több ezer „haszontalan" levelet küldenek, s ezáltal az illető levelezése gyakorlatilag megbénul, mivel folyamatosan kapja a (percenként akár több száz) e-mailt.

A mailbombázók nem jelentenek közvetlen veszélyt az internet-használók adataira vagy a számítógéprendszereikre, inkább csak idegölők és zavarók. Ugyanis elég időigényes – és drága – lehet, ha az embernek hirtelen 5000 nem kívánt mailt kell törölnie a postafiókjából.

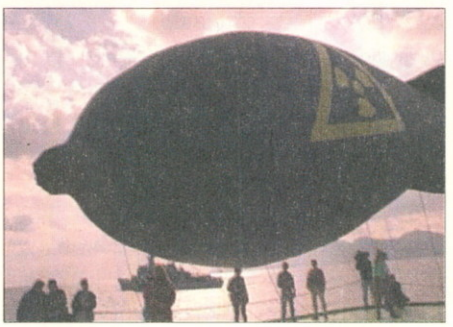
Az e-mail bomb

A levélbomba nagyon-nagyon csúnya dolog, de iszonyúan hatásos... - olvasható az egyik legismertebb levélbomba-program készítőjének a weboldalán. Milyen igaz! A „profi" levélbomba szoftverek automatikusan változtatják a feladót, a tárgyat és a tartalmat is: ezáltal a levelezőprogramokba épített szűrők *(e-mail filterek)* nem képesek különválasztani a valódi és a bombázott e-maileket. Ha levélbombát kapunk, sajnos sok lehetőségünk nincs a védekezésre: vagy kiválogatjuk a sok ezer e-mail közül az „igaziakat", vagy pedig letöröljük az egész mailboxot – persze ezzel a rendes levelezésünk is elvész. Az egyetlen parányi segítség, hogy a szűrőbe beírjuk azoknak az e-mail-címeit, akikkel biztosan és nap mint nap levelezünk – pár e-mailt megmenthetünk ezzel a módszerrel.

A legtöbb mailbomba program nagyon fejlett és hatékony, a *Kaboom* például több klónt hoz létre saját magából, és különböző levelezőprogramokként azonosítja magát a szerver felé – ezáltal még a szolgáltató mail-szerverét is megtéveszti.

Ahogy a hacker látja...

„Általában azt kell beírni, hogy kinek küldjétek, meg milyen kamu szerveren keresztül, és persze hogy hány darabot. Ja és persze arra szolgálnak, hogy tönkretegyük vele a páciens mailboxát. Mivel megtelik, nem tud újabb üzeneteket fogadni. Vannak olyanok is, amelyek csak egy párat küldenek, és utána ott kisűrítik/szétterjesztik magukat több 100 Mbájtra."- Dodge Viper



Olyan mint a levélbomba – csak rosszabb...

A mailbombázók sajátos képességei tehát nemcsak abban nyilvánulnak meg, hogy szinte egyidejűleg hallatlanul nagy számú mail-t tudnak küldeni a kívánt címre, hanem abban is, hogy *névtelenek maradnak*, vagy választás szerint meg tudnak adni egy hamis feladó-címet is.

A mailbombázáshoz a támadók számos programból választhatnak. Nehéz felmérni, hogy mennyire van stratégia a mailbomba-támadások mögött. Egy egyedi felhasználónak főleg az idejét rabolhatják a bombázással, s akkor bosszanthatják, ha tudják, hogy egy fontos mail-re vár. Ezt ugyanis, mivel a mailbox a támadás miatt túltelítődik, a szerver vissza fogja utasítani. Egy ilyen támadás azonban akár pénzügyileg is érinthet kisebb cégeket, amelyeknek fontos kommunikációs eszközt jelent az internet.

A Nuke

A Nuke vagy a „nuke-olás" nagyon egyszerű dolog, viszont roppant idegesítő. Tulajdonképpen csak idegesítő és nem kifejezetten ártalmas. A Nuke (= fagyasztani, kilőni) lényege, hogy az áldozat gépének egy bizonyos portjára (portjaira) olyan adatokat küldenek, amitől annak a gépe lefagy, megbénul. Alkalmazható szerverekre, de vannak a Windowst lefagyasztó verziók is. A teendő csak annyi, hogy meg kell tudni az áldozat IP-címét vagy gépének a nevét: a Nuke programok ugyanis semmi mást nem kérdeznek. Elég beírni az IP-címet, rábökni a *Nuke it!* gombra – és ha minden működik, akkor a megtámadott gép lefagy. Persze ha valakinek egyszer-kétszer lefagy a számítógépe az nem gond, de képzeljük el, hogy például az irodai gépünket a nap mind a 24 órájában folyamatosan nuke-olja valaki... Gyakorlatilag bekapcsoljuk, elindul, majd lefagy – és ez megy egész nap. Dolgozni lehetetlen, a gépet átnéző szakember pedig nem lát semmit – hiszen a gépnek „semmi baja".

A leghíresebb Nuke szoftver a *WinNuke* volt – ezzel a NetBios hibáját kihasználva a windowsos gépeket lehetett „kékre" kifagyasztani, egészen addig, amíg a Microsoft nem orvosolta a hibát. (Azóta már nem hatásos.)

A legtöbb Nuke szoftver ellen ma már védekeznek az internet-szolgáltatók, no de azért vannak a hackerek, hogy újabbnál-újabb Nuke programokat írjanak☺. Nuke-olni tehát mindenkit lehet, hál' istennek a védekezés nagyon könnyű ellene: egész egyszerűen tegyünk a gépünkre egy tűzfalprogramot, és a Nuke máris hatástalan. ■

FAX MEGRENDELŐLAP

Computer Panoráma Kiadói Kft.
Terjesztési Osztály
1091 Budapest, Üllői út 25.
Tel.: 456-69-63

Fax: 456-69-70

Igen, utánvéttel megrendelem az alábbi különszámokat és könyveket:

- ❒ 2003/14 CAD/CAM (795 Ft)
- ❒ 2003/12 Projekt Menedzsment (695 Ft)
- ❒ 2003/11 Notebook (695 Ft)
- ❒ 2003/10 Cad/CAM (695 Ft)
- ❒ 2003/9 Nyomtatók (695 Ft)
- ❒ 2003/8 Digit Fotó (695 Ft)
- ❒ 2003/7 Mobil Világ (495 Ft)
- ❒ 2003/6 Adatbiztonság (695 Ft)
- ❒ 2003/5 Download (695 Ft)
- ❒ 2003/4 PC-Házimozi (1990 Ft)
- ❒ 2003/3 CAD/CAM (695 Ft)
- ❒ 2003/1 Tesztgyőztesek (495 Ft)

- ❒ PC & MOZI (3990 Ft)

- ❒ 300%-os tuning I. kötet (2990 Ft)
- ❒ 300%-os tuning II. kötet (2990 Ft)

- ❒ 300%-os tuning I. és II. kötet (kedvezményesen csak 4990 Ft)

- ❒ Hacker, cracker, warez (4990 Ft)
  - ❒ Kérem, a szerző által dedikált pédányt küldjenek.
- ❒ PC-doktor (3990 Ft)

- ❒ CD-írás A-tól Z-ig (3490 Ft)

Tájékoztatjuk, hogy személyes adatait csak arra használjuk, hogy akcióinkkal kapcsolatban megkeressük Önt. Adatainak felhasználását addig tekintjük folyamatosnak, amíg levélben vagy telefonon nem kéri annak törlését. Amennyiben adatai felhasználásához a későbbiekben nem járul hozzá, kérjük, ezt jelezze!

SZÁMLÁZÁSI CÍM:

Cégnév: _____

_____

Ir.sz: _____ Helység: _____

_____

Út/utca/tér: _____

_____,

hsz. _____, em./ajtó: _____ / _____

Telefon (napközben): 06 _____

E-mail: _____

_____

Kérjük, a kézbesítés megkönnyítése és a gyors ügyintézés érdekében minden adatot feltétlenül adjon meg!

POSTACÍM:

Cégnév: _____

_____

Ir.sz: _____ Helység: _____

_____

Út/utca/tér: _____

_____,

hsz. _____, em./ajtó: _____ / _____

Telefon (napközben): 06 _____

Mobilszám: 06 _____

dátum _____ aláírás _____

A megrendelés átfutási ideje körübelül 2 hét.
Régebbi különszámaink megrendelhetők weboldalunkon. Internet: www.computer panorama.hu/megrendeles, E-mail: **megrendeles@cpanorama.hu**
A megrendelt különszámokat utánvéttel küldjük, áraink a postaköltséget nem tartalmazzák! (A postaköltséget az érvényes postai díjszabás szerint számoljuk.)

Folpakker és Netbus

A trójai falovak – tartja a közvélemény – az internet legveszélyesebb és legtitokzatosabb programocskái. De vajon mit mond egy igazi hacker a trójaiakról? Cikkünkben a Computer Panoráma kiadó nagysikerű könyvéből idézünk egy tanulságos interjút.

[...] Huy befejezte a sört, és elvonult a garázs legsötétebb zugába: B.-vel susmognak és instalállnak, valószínűleg készül az első wargames szerver. Mivel nem akarom őket zavarni (végül is egy kívülálló vagyok) kinn maradok a lócán. Szerencsére Zoli nemsokára megjelenik, hogy begyűjtse kintfelejtett notebookját, én pedig rögtön lecsapok a srácra. Legújabb ismerősöm elég szószátyárnak tűnik szakmai dolgokban.

– Tanítgass kicsit a trójai programokról: mindenki csak azt mondja, hogy „beviszel egy trójait" és hasonlók.. De engem az érdekel, hogy hogyan?

– Hát igen, a trójai programok ezerfélék lehetnek és millióféle dologra képesek. Egy trójaival logolhatom, hogy milyen billentyűket ütsz le, de lefagyaszthatom az egeredet is, ha akarom. Készíthetek pillanatképet a desktopodról, vagy teljesen átvehetem az ellenőrzést a vinyód felett... Szóval összetett téma. Ha valaki nagyon profi, akkor még a CD-meghajtódat is kinyitja egy trójaival, hehe...

– Na ne... Te is tudsz ilyet?

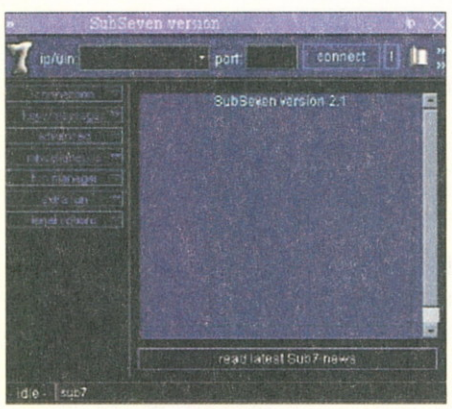
– Persze. De Huy többet tudna mesélni erről.

– De mégis? Hogyan működik? Azért te is értesz hozzá gondolom...

– Hízelegsz?

– Igen...

– Jó, jó. Szóval a trójaiaknak két népszerűbb verziójuk van, a *Subseven* és a *Netbus* – ez nem a trójai program neve,



Az egyik legnépszerűbb trójai program

hanem az eljárásé, amivel működik. Ebből az egyszerűbb a Netbus, szóval erre tudok példákat, ha gondolod...

– Gondolom. Írom...

– Jó. A Netbus trójai is két részből áll (mint általában mindegyik trójai): a kliensből és a szerverből. A szerver a trójainak az a része, amelyet a másik gépen valahogy installálni kell – ha ez megvan, akkor máris tudunk „gonoszkodni".

– De hogy installálod? Gondolom nem személyesen...

– Hihi, persze, hogy nem. Szóval a feladat: installáljuk a trójait valaki gépére. A legegyszerűbb módszer, hogy a trójait elküldöd egy levélhez csatolva, és ráveszed a felhasználót, hogy indítsa el a csatolmányt. Ezt csinálhatod úgy, hogy egy ismerőse nevében küldesz egy „fake" mailt, benne egy *akármi.exe-vel* és egy kis szöveggel, hogy: „találtam egy aranyos képernyővédőt, nézd meg..." vagy ilyesmi. Esetleg álcázhatod URL-nek is a csatolmányt, a *.com* kiterjesztést kihasználva: hiszen egy program, ami a *humoroskepek.com* névre hallgat, tisztára úgy néz ki, mint egy internetcím. A legbiztosabb, ha a trójait „becsomagolod", azaz ha az áldozat elindítja a humoros képernyővédőt, akkor az tényleg csinál valamit (egy humoros képernyővédőt☺), így nem is lesz „gyanús".

– De hogy csomagolod be?

– Hát folpakkba☺! Szóval komolyan: rengeteg kis utility van, amely erre való. Fogja neked a trójait, és bármilyen szabályos futtatható (exe) fájlba beteszi - pitty-putty, egy másodperc. Ilyen program például a ******.

Nem mindig biztos

Nem biztos, hogy a képfájl valóban képfájl.

„Írd a parancsfájlt az „akarmi.jpg.txt" - be, helyezd néhány sorral elé vagy néhány sorral utána a kép kódját. Ezután nevezd át az *akarmi.jpg.txt-t akarmi.jpg.scf-re,* az .scf rejtve marad. Ezután küld el az áldozatodnak, és amikor futtatja a fájlodat, végrehajtódik a parancsfájl. Ez nem nyitja meg a képet, csak a te parancsfájlodat futtatja." – B$H

Néhány jó tanács

Ha a következő fájlkiterjesztéssel kapunk valamit, akkor semmiképp se indítsuk el, bárkitől is jön az e-mail:

- <valami>.com
- <valami>.exe
- <valami>.vbs
- <valami>.txt.vbs
- <valami>.swf

Amit elindíthatunk, de nem teljesen biztonságos:

- <valami>.doc
- <valami>.rtf
- <valami>.xls

És végül ami biztonságos:

- <valami>.jpg
- <valami>.avi
- <valami>.gif
- <valami>.bmp
- <valami>.tiff
- <valami>.mpg
- <valami>.mpeg
- <valami>.mp3

– Konkrétabban?

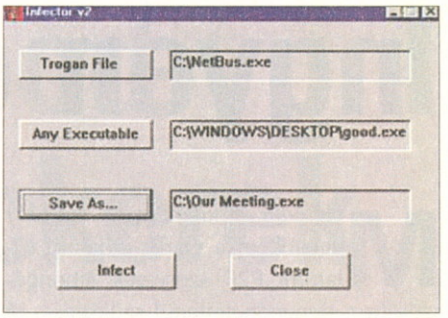
– Mondjuk tudod, hogy az áldozat nagy sakkrajongó. Szóval fogsz egy 30K-s sakkprogramot *(chess.exe)*, és veszed a kis trójaidat *(netbusserver.exe)*: a kettőből a ***** nevű joiner csomagol neked egy fájlt. A kész cuccot kimented *chess.exe* néven: a különbség annyi lesz, hogy a 30K-s chessből mondjuk 50K lett. Nagy ügy! A kolléga megkapja a mailt, mellette egy kis szöveg, hogy „Helló sakkrajongó barátom! Ezt a levelet a sakkrajongók.hu küldi neked – ha meg tudod verni ezt a sakk-algoritmust, akkor nyersz egy hangszórót! – bla, bla, bla". Naná, hogy rányom: erre elindul a sakkprogram, ő meg vagy megveri, vagy nem (kit érdekel?). A lényeg, hogy miközben ő sakkozgat, a trójai már fel is installálta magát szép csendben.

– És mit csinál utána a trójai?

– Hát, amire be van programozva. A legegyszerűbb trójai megfigyeli az áldozatot, azaz azon felül hogy a hackernek elküld minden adatot a célgépről (felhasználó neve, IP-címe, hardver, szoftverek a gépen, mi van a vinyón stb.) még arra is képes, hogy „szóljon" a hackernek, hogy a célgép mikor van az interneten és mikor nincs. Szóval, lehetsz nyugodtan dial-up-os is, nem számít: a hacker tudja, hogy most a neten vagy-e vagy sem. Trójait persze bevihetsz hírcsoporton, IRC, ICQ-n vagy weben keresztül is: a lényeg, hogy bent legyen és valahogy elinduljon.

– És mit lehet tenni ez ellen?

– Egy hozzáértő és óvatos felhasználó tudja, hogy soha, semmit ne indítson el, amit nem ő telepített. Szóval, még ha az anyukádtól is jön az „indítselkisfiam.exe", azt is töröld le rögtön. És persze a jobb memóriarezidens vírusfigyelők is képesek „belekukkantani" a csatolmányba, s ha nagyon gyanús a kód néhány eleme, akkor észreveszik. De igazán kivédeni nem lehet, mert trójait be lehet vinni a webről is, egyszerű JAVA-s verzióban, azután vannak ugye a makrók a Word doksikban, az Excelben... Trójai mindenben lehet. Az egyik legnépszerűbb trójai a *BO*: viszonylag könnyen használható és elég sok mindent tud.



Egy „joiner" azaz trójai-csomagoló program, működés közben

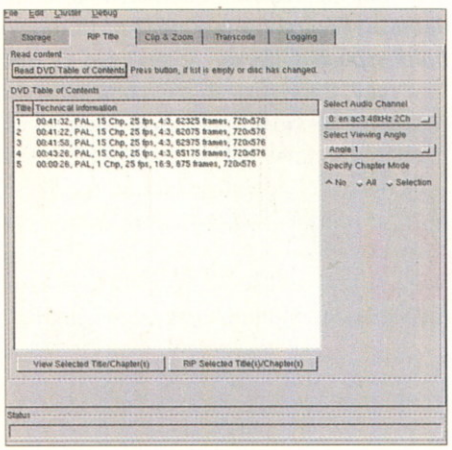
– Akkor mi a tuti ellenszer?

– Hát az, ha soha nem mész fel a netre☺! A tűzfal általában beválik, de nem mindig. A legtöbb, amit tehetsz, hogy csak a nagyon megbízható forrásból származó fájlokat indítod el. Egyedül a képekbe nem lehet trójait ágyazni, szóval JPG, GIF meg ilyesmi állományokat elindíthatsz. Persze ne úgy nézzen ki, hogy *britneyspears-GIF.exe*. ■

Ingyen és bérmentve

A warez-szervereken szinte mindig van pár szár Gbájtnyi MP3-állomány – a zene megszokott és gyakori a szoftverkalózkodásban. Persze nem kerülhették el a sorsukat a filmek sem: az illegális szoftverforgalom felét, a játékok és egyéb szoftverek mellett, mára már a különböző DivX filmek és DVD-rippek teszik ki.

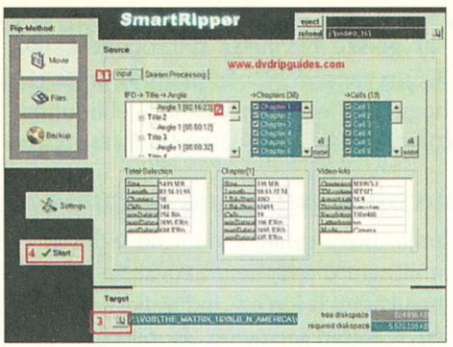
Megfelelő kitartással, amely egyébként a warez-oldalak, valamint P2P szerverek átböngészéséhez elengedhetetlenül szükséges, rá lehet bukkanni a letölthető, crackelt másolatokra. No persze nem is olyan könnyű egy DVD teljes adatmennyiségét kb. 700 Mbájtra redukálni ahhoz, hogy egyáltalán rákerülhessen a hálóra, és onnan CD-re lehessen írni. Néhány időigényes munkafolyamatra ugyanis ehhez is szükség van. Ami meglepő: már olyan filmeket is másolnak, amelyek még Amerikában sem kerültek DVD formájában kereskedelemi forgalomba. Megfelelő lelkesedésű emberek lefilmezik a vásznon látottakat, és azután feldolgozzák ezeket.



DVD-rippelés – csak egy gombnyomás...

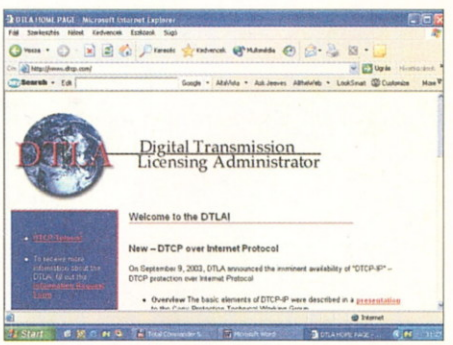
Az ipar természetesen megpróbálja nem tétlenül nézni az effajta tevékenységeket. A filmipar a DVD bevezetésével egyidejűleg kifejlesztett egy országonként eltérő kódot. A kód megakadályozza, hogy egy amerikai filmet (Code 1) megnézhessenek Európában (Code 2) vagy Ausztráliában (Code 4), amennyiben a DVD-meghajtókat és a -lejátszókat az egyes országokban egy regionális kódra állítják be.

A nagy amerikai filmstúdiók ezen felül bevezették a *Content Scrambling System* (CSS) elnevezésű másolásvédelmi rendszert is, és megbízták a *Copy Control Association-t* (másolást ellenőrző társaságot) (DVD-CCA), hogy fejlessze ki a másolásvédelmi módszert. Az *Intel*, a *Sony*, a *Toshiba*, a *Hitachi* és a *Matsushita* vállalatokat magába tömörítő szövetség set top boxok és digitális videofelvevők számára fejlesztett ki egy új biztonsági standardot, a *DTLA-t (Digital Transmission Licensing Administrator)*, és jelenleg azzal próbálkozik, hogy a másolásvédelmi rendszert eladja a stúdióknak. A jogtulajdonosok által bevezetett intézkedések azonban nem gördítenek valós akadályokat a kalózok útjába. Ahhoz, hogy az országonként más és más kódot kijátsszák, felhasználják a DVD-meghajtók és -lejátszók azon tulajdonságát, hogy ötször változtathatnak kódot, mielőtt ráállnak a véglegesre.



SmartRipper: szinte mindent beállíthatunk

Az interneten fellelhető apró, ingyenesen hozzáférhető *DVD Genie* elnevezésű eszköz pedig egyszerűen visszapörgeti a meghajtó vagy a lejátszószoftver számlálóját. Némely cracker már olyan messzire is elmerészkedik, hogy a készülék Flash-ROM-ját egyszerűen átírja, „0"-ra állítva a kódot. Egy évvel ezelőtt a CSS másolásvédelmi rendszer feltörése keltett riadalmat. A DeCSS program őrült sebességgel terjedt szét az interneten. A filmipar végül sikeresen keresztül vitte, hogy tilos legyen letölteni a DeCSS-t, vagy linkeken keresztül utalni a megfelelő oldalakra. A *The Hackers Quarterly* elnevezésű magazin röplapok segítségével mindmáig harcol a rendelet ellen. Időközben az interneten keresztül már hozzáférhető az ingyenes *Smart Ripper* program, amely meglehetősen kényelmesen intézi a DVD-k másolását és dekódolását. Ezen felül azonban ahhoz, hogy az ember internetre alkalmas méretűre zsugorítson egy filmet, szükség van még néhány munkafolyamat elvégzésére.



Az új biztonsági szabványról az interneten is olvashatunk

A FlaskMPEG és a DivX-Codec segítségével az adatokat az általánosan kompatibilis MPEG-4 formátumba kell átalakítani, majd például a VirtualDub-bal a hangot és a képet lehet optimalizálni.

Nem elegendő tehát semekkora igyekezet arra nézve, hogy a filmkalózokat eltántorítsák erősen megkérdőjelezhető tevékenységüktől. Nem ijesztik el őket a részint jelenleg is függőben levő „ipar kontra illegális másolók" perek. Többé kevésbé legálisan, illetve illegálisan készülnek a másolatok, crackelnek, letöltenek - mindent megtesznek, amit csak elbír a merevlemez. ■

Hollywood és a hackerek

Régóta tudjuk, hogy az Egyesült Államokban (és persze máshol is) mindent megfilmesítenek. Sorsukat a hackerek és az egyéb számítógépes fenegyerekek sem kerülhették el, hiszen a téma érdekes, izgalmas és titokzatos. A hacker-témát feldolgozó filmek között vannak jók, sőt kiemelkedők is – persze a többségük amolyan „hollywoodi", azaz semmi köze a valósághoz. Az érdekes témáról Réz András, az ismert filmesztétát faggattuk.

Computer Panoráma (CP.): A filmekben szinte mindent másképpen ábrázolnak, mint ahogyan a valóságban láthatjuk. A számítástechnika (szoftverek, vírusok stb.) megjelenítése azonban még az átlagosnál is jobban elrugaszkodik a valóságtól... Ön szerint mi lehet az oka ennek?

Réz András (R. A.): Nem hiszem, hogy a világ legizgalmasabb látványa lenne, amikor valaki éjszakákon át ül a billentyűzet előtt, és csak azért kel fel a helyéről, hogy kiürítse a hamutartót, vagy a pizzafutártól átvegye a kaját és az üdítőt. *Pierre-Paul Renders* filmjét, a *Szerelmes Thomas*t is csak azért élvezzük, mert nem a főhőst látjuk, hanem a képernyőjén mindazokat, akikkel valamilyen kapcsolatba kerül. Amúgy meg a tömegfilm arra van kihegyezve, hogy a számítástechnikában, az IT-világban nem túl járatos néző is együtt tudjon haladni vele. És arról sem szabad megfeledkeznünk, hogy az IT, a digitális technológia misztifikálása elemi érdeke a tömegfilmnek: ha nem tudod, hogyan működik, a forgatókönyvi lelemény bármit felpakolhat rá. Ha kedve tartja, kitalálja a Szupergonoszt, aki sitty-sutty megcrackeli az egész világot. Vagy emlékezzünk *A hálózat csapdájára*. Hálás ötlet, hogy valakit el lehet tüntetni minden adatbázisból, nem? Még akkor is, ha a valóságban ez nem tűnik igazán kivitelezhetőnek. Néha az az érzésem, hogy a hálózatokat egyre inkább egyfajta Big Brotherként fogják fel – orwelli értelemben. Bennük újraírható akár a történelem is (ld. pl. *Stephanie Benson* regényét, az *Áldozatok a könyvtárban*-t). A tömegfilm, a műfaji film tehát nem pontosságra, hitelességre törekszik, hanem egyfajta metaforaként, allegóriaként alkalmazza a számítógépekre épülő kultúrát. És ez már az Űrodisszeiában is így volt...

CP.: Lehetséges, hogy ez a képi és technikai ábrázolás (háromdimenziós csillogó-villogó vírusok a képernyőn) idővel közelít majd a valósághoz, vagy megmarad a dolog olyannak, amilyen?

R. A.: Miért kellene közelíteniük a valósághoz? A fantasy-tól sem várjuk el, hogy valóságos lényekből építkezzen, a horrorfilmnek is megvannak a szupernaturális mozzanatai, a *Tigris és sárkány* sem korlátozza magát az ember által valóságosan végrehajtható mozgássorokra.

CP.: Beszélgessünk kicsit a „hackeres" filmekről! Mint esztétának, mi a véleménye az ilyen (TRON, Wargames, AntiTrust stb.) filmekről?

Egy igazi filmklasszikus: a TRON

R. A.: Filmesztétaként nem vállalkoznék rá, hogy egy kalap alá vegyem valamennyit, és úgy alkossak véleményt. Leginkább Mátrix-hívő vagyok, de belefér egy kis *Johnny Mnemonic*, de a *TRON* is. Ráadásul itt különböző műfajú filmek keverednek egymással. A számítástechnika, a „rendszer", a „hálózat" ugyanúgy része lehet egy akciófilmnek vagy egy kémfilmnek, mint egy katasztrófafilmnek.

CP.: Van esetleg kedvence a számítástechnikai témájú filmek közül?

R. A.: A fentiekből kiderülhetett, hogy a Mátrixot tartom az egyik legizgalmasabb alkotásnak.

CP.: Meglepődve tapasztaltuk, hogy a hackerek között kultuszfilmnek számít Vincenzo Natali „A Kocka" című filmje, annak ellenére, hogy a téma nem igazán „hackeres." Mi a véleménye erről a filmről?

R. A.: Kedvelem, de nem vagyok elájulva tőle. Nekem a Kocka egy sajátos tézis. Nagyon letisztult, nagyon steril. Ha valaki szeret zárt rendszerekben, véges univerzumokban gondolkodni, annak igazán jó kaland. Engem azért nem nyűgözött le annyira, mert világos volt, hogy ebből a világból a film nem fog kilépni, és a pontosan megtervezett modellből nem lehet kitörni. De azért a film rendben van.

A Mátrix még nem klasszikus, de könnyen azzá válhat

CP.: Tudom naiv kérdés, de mégis: ha választani kellene, melyik filmben sikerült eddig legjobban ábrázolni a „hackert" és a számítógépekbe való betörést - Ön szerint?

R. A.: Fogalmam sincs. Más a *Komputerkémek,* a 007-es típusú filmek világa, a *Y2K*-filmek (pl. *Briliáns csapda),* más a *Zaklatás* és megint más a cyberpunk. Valójában egyik sem hiteles, de attól még nagyon fogyaszthatók.

CP.: Tegyük fel: valaki egyszer „földhöz ragadt" vagy realista módon ábrázolná a hackereket, a számítógépekbe „poénból" betörő, izzadt trikós, lövöldözni nem tudó, cseppet sem jóképű fiatalok képében... Vajon bukás lenne?

R. A.: Ja, dokumentumfilm... Garantált bukás lenne, már csak azért is, mert a fényviszonyok tudvalévőleg nem kedveznek a kamerának. Bár azt nem tartom kizártnak, hogy valaki készítsen egy jó kis rétegfilmet (art filmet) egy olyan figuráról, aki totális antihős, de a hálón mégis szuperhősként éli meg önmagát.

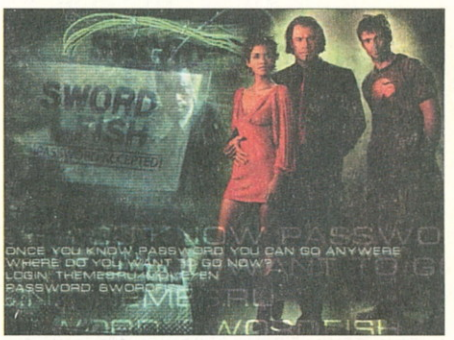
CP.: Hollywood nagyon óvatosan (vagy sehogy sem) foglalkozik a Microsoft, a monopólium, Bill Gates, a felhasználók adatvédelme és „kiszolgáltatottsága" jellegű témákkal. Ez merő véletlen lenne? Hálátlan a téma, netán Hollywood óvatos?

R. A.: A már említett *A hálózat csapdájában* azért foglalkozott ezzel a kérdéssel. Emlékszünk ugye, hogy bizonyos „Gatekeeper"-ről van benne szó, és ezt a célzást mindenki értette, aki a számítástechnika körül sertepertélt.

CP.: Ön szerint mit hoz a jövő? A számítástechnika (hackerkedés...) vonzereje megmarad a filmekben, vagy idővel érdektelenné válik?

R. A.: Egyre vonzóbb lesz, bár a hangsúlyok áthelyeződhetnek. Ma már az Echelonnal kapcsolatos kérdések – ld. Big Brother's watching you – jönnek elő, magyarán az a probléma, hogy mega-adatbázisok keletkeznek, hogy állandóan trackelnek, azaz a saját géped figyel téged. Azt hiszem, hogy az ezzel kapcsolatos szorongásainknak meg kell jelenniük a tömegfilmekben, s ezért a téma nem fog kihullani. Sőt, van egy sor vadonatúj kérdés, amely inkább lökést ad neki: halhatatlanság, nanotechnológia, IP2, a világon működő processzorok számának brutális növekedése - akár 30 milliárd chipig...

CP.: A beszélgetés végére egy idevágó kérdés: milyen a kapcsolata a számítógépekkel és az internettel? Használja, esetleg rajong érte, netán csak elviseli?



Kardhal: Ha tudod a jelszót, bárhova mehetsz...

R. A.: Elemi munkaeszközöm. Bár kétségtelen, hogy döntő módon szövegeket gyártok, de ma már a gép nélkül nagy bajban lennék, hiszen már rászoktam arra, hogy mindent ebben rendszerezzek. Azután persze kommunikációs eszköz is. Ha nem lehetne ördögi sebességgel cserélni a szövegeket, képeket, a munkám töredékét tudnám csak elvégezni. Ma már az egyetemen a hallgatóim is a **www.rezandras.hu**-n kapják meg a házi dolgozat témáját, az ottani „postaládába" dobják be az elkészült dolgozatokat. A szakdolgozati konzultációk is többnyire „emilben" zajlanak. A megjelent cikkeimet is ide rakom fel, hogy ha valakit érdekel, elolvashassa. És persze azt sem szabad elfelejteni, hogy a világháló elképesztő méretű könyvtár is. Néha még játszani is szoktam. Van úgy, hogy rákattanok valami jó kis FPS-re (kedvenc műfajom), és akkor pár napig bizony függő vagyok. Ezzel együtt – töredelmesen bevallom – a PC-m képességeinek csak nevetségesen kicsiny hányadát használom ki. ■

Hozza ki számítógépéből a maximumot!

hardvertuning

PC-építés, PC-tuningolás, segédprogramok

- Saját PC, de hogyan?
- Szerelési útmutató
- Alaplap- és processzorcsere
- A CPU-frekvencia növelése
- A meghajtók tuningolása

szoftvertuning

szoftvertuningolás, segédprogramok

- Telepítési problémák megoldása
- Busz- és memóriatuningolás
- Egyéni beállítások átvitele
- Tuningolás szoftver-cache-sel
- Illesztőprogramok frissítése

A két kötet 5980 Ft helyett csak 4990 Ft!

300%-os szoftvertuning CD-melléklettel
Ára: 2990 Ft

300%-os hardvertuning CD-melléklettel
Ára: 2990 Ft

Megrendelését 2 héten belül teljesítjük! A megrendelt könyveket utánvéttel küldjük, áraink a postaköltséget nem tartalmazzák!
(A postaköltséget az érvényes postai díjszabás szerint számoljuk.)

Telefon: 456-6963, Fax: 456-6970, Internet: www.computerpanorama.hu/tuning
E-mail: megrendeles@cpanorama.hu

Ilyen még nem volt!

Megdöbbentő vallomások a hazai hackerektől
Crackerek beszélnek életükről és munkájukról
Felfedjük a warez-világ legféltettebb titkait!

Hacker, cracker, warez

A számítógépes alvilág titkai

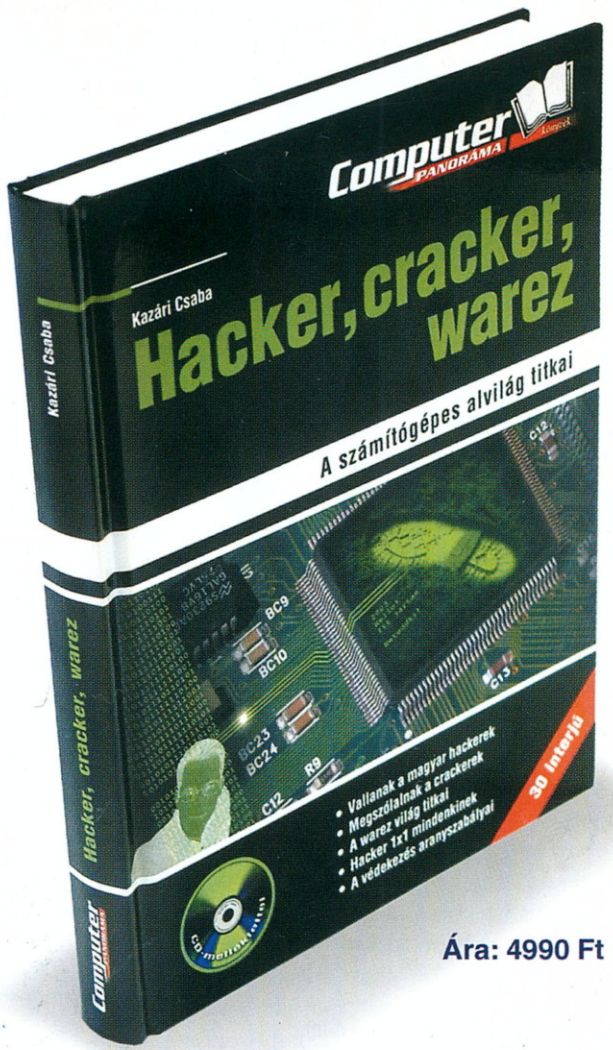
Vallanak a magyar hackerek
Megszólalnak a crackerek
A warez világ titkai
Hacker 1x1 mindenkinek
A védekezés aranyszabályai

"Feltörni valamit? Egyáltalán nem nehéz. A nehéz az, hogy közben és utána is észrevétlen tudj maradni."

"Aki tud programozni, az fel is tud törni bármilyen szoftvert - tulajdonképpen csak hozzáállás kérdése, hogy programozó lesz az ember vagy inkább cracker."

"Most komolyan - el tudod képzelni, hogy egy tizenéves kölyök játékprogramot vásároljon?"

CD-melléklettel



Ára: 4990 Ft

Telefon: 456-6963, Fax: 456-6970
Internet: www.computerpanorama.hu/hacker
E-mail: megrendeles@cpanorama.hu

Megrendelését 2 héten belül teljesítjük!
A megrendelt könyveket utánvéttel küldjük, áraink a postaköltséget nem tartalmazzák!
(A postaköltséget az érvényes postai díjszabás szerint számoljuk.)

Rendelje meg most!