A Windows tűzfal precíz nyilvántartást vezet a hálózati kapcsolatokról

nyomtatómegosztás bejegyzést, majd kattintsunk a *Szerkesztés* gombra. Most megnyílik a *Szolgáltatás módosítása* panel.

Itt azt láthatjuk, hogy az engedélyezett szolgáltatáshoz négy portnak kell nyitva lennie, azonban csak az úgynevezett alhálózat számára. Az ADSL-en, ISDN-en vagy az analóg modemen keresztül létrejött internetkapcsolatok esetében azonban az alhálózat a teljes internetre vonatkozik. A betárcsázás után eszerint a számítógép tárva-nyitva lenne.

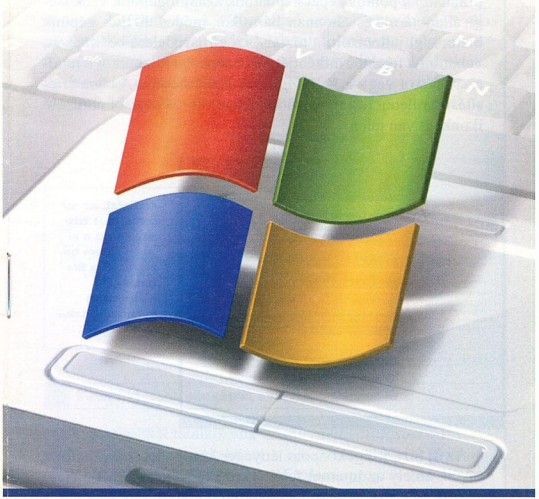
Segítséget úgy kaphatunk, ha egymás után mind a négy portot kijelöljük, és a *Hatókör módosítása* gombra kattintunk. A hasonló nevű ablakban jelöljük ki az *Egyéni lista* bejegyzést, majd adjuk meg itt a helyi hálózatban található számítógépek IP-címét, amelyek a számítógépünk megosztásaihoz hozzáférhetnek. Egyszerűbb a dolog, ha egyből a teljes LAN-t engedélyezzük. A helyi hálózatunk hálózati címének meghatározásához kattintsunk kétszer a *Tálcán* található *Helyi hálózati kapcsolat* ikonjára, és nyissuk meg az *Állapot* ablakban a *Támogatás* fület.

Az egymástól három ponttal elválasztott négy számból álló IP-címet adjuk meg az *Egyéni lista* alatti mezőben. Az IP-cím utolsó számát (nem számjegyét!) helyettesítsük egy 0-val. Közvetlenül ezután írjunk be egy perjelet (/), majd adjuk meg az alhálózati maszkot. Amennyiben az alhálózati maszk 0.0-ra végződik, helyettesítsük az IP-cím harmadik számát is egy 0-val. Kattintsunk az *OK* gombra, majd végezzük el ugyanezt a módosítást mind a négy porton.

Ezzel megakadályozzuk, hogy az internetről számítógépek férjenek hozzá a nyitott internetkapcsolatunkon keresztül a PC-nk vagy a laptopunk megosztásaihoz.

Windows XP 2. szervizcsomag

Telepítés, tapasztalatok, tippek



Nemrég jelent meg a *Microsoft* eddigi legnagyobb, legátfogóbb javítócsomagja, a *Windows XP SP2*. Sokan vannak, akik tüstént telepítették is, és ugyancsak sokan vannak, akik még csak ezután fogják telepíteni. A szervizcsomag segítségével biztonságosabb munkakörnyezetet alakíthatunk ki a számítógépen: javíthatjuk a gép (és az operációs rendszer) védelmét a vírusok, a férgek és a hackerek ellen, ezenkívül új technológiák várnak bevetésre, amelyek kényelmesebb böngészést és kommunikációt tesznek lehetővé. A szervizcsomag új eszközeivel könnyebben felügyelhetők a biztonsági beállítások, és folyamatosan letölthetők a legújabb frissítések, amelyekkel napra készen tarthatjuk az operációs rendszerünket.

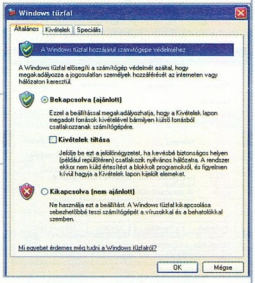
Windows Biztonsági központ

A 2. szervizcsomag legfőbb újdonsága az úgynevezett *Windows Biztonsági központ,* amelynek segítségével minden pillanatban pontos képet kaphatunk számítógépünk védettségi állapotáról, és ahonnan bármikor módosíthatjuk gépünk biztonsági jellemzőit: a tűzfal és a vírusvédelem beállításait, valamint a frissítés mikéntjét. A Biztonsági központot a rendszertálcáról vagy a *Vezérlőpultról* is elérhetjük. A tálca értesítési területén (a jobb alsó sarokban) vörös pajzsot ábrázoló ikonként van jelen.

A tűzfal, az automatikus frissítések és a vírusvédelem beállításait a Biztonsági Központon keresztül szabályozhatjuk

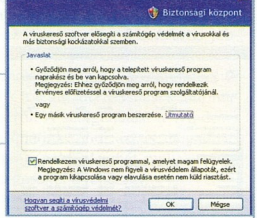
Az új biztonsági központ lényeges komponense a *Windows tűzfal,* amely az internet felől érkező fenyegetésektől – vírusoktól és rosszindulatú behatolóktól hivatott megvédeni a számítógépet. A tűzfal beállításait a *Vezérlőpulton* keresztül, a *Tűzfal* ikonról érhetjük el. A védelem természetesen akkor ér valamit, ha a tűzfal bekapcsolt állapotban van.

A biztonság érdekében ne feledjük el bekapcsolni a tűzfalvédelmet



A Biztonsági központból a vírusvédelem állapotát is figyelemmel kísérhetjük. A víruskereső szoftverek többsége jól együttműködik a Biztonsági központtal, vagy ha mégsem, a központ figyelmeztetést küld a vírusvédelem hiányáról. Ilyenkor ki is kapcsolhatjuk a riasztást, és a továbbiakban magunk felügyelhetjük a gép vírusvédelmét.

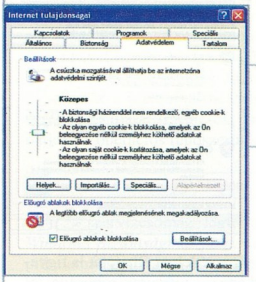
A riasztásokat kikapcsolhatjuk, ha magunk akarjuk felügyelni a vírusvédelmet



Biztonságosabb böngészés és levelezés

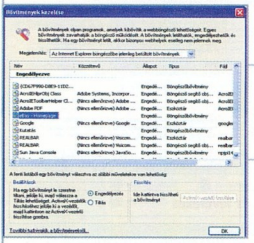
Újdonságokkal találkozunk az *Internetbeállításokban* is. A legfontosabb talán ezek közül a bosszantó *előugró ablakok blokkolása* a *Microsoft Internet Explorer* programban. Ezt a funkciót bekapcsolva megakadályozhatjuk, hogy egy

webhely engedély nélkül megnyisson egy előugró ablakot, és ezzel akadályozza a zavartalan böngészést. Előugró ablak blokkolásakor figyelmeztető üzenetet kapunk, ám egyetlen kattintással úgy is dönthetünk, hogy engedélyezzük a szóban forgó ablak megnyitását a képernyőn.



Zavartalanabbul böngészhetünk, ha letiltjuk az előugró ablakokat az Internet Explorerben

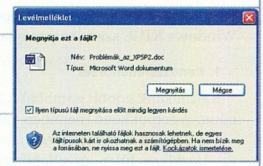
Ugyancsak az Internet Explorer használhatóságát javítja az új *Bővítménykezelő* is, amely segít kordában tartani a böngészőprogramba betöltött különféle bővítményeket, például az oly sok bosszúságot okozó *ActiveX* vezérlőket. A listában szereplő bővítmények bármelyikét tetszés szerint engedélyezhetjük vagy letilthatjuk, tovább növelve az internetezés kényelmét és biztonságát.



Az Internet Explorer Bővítménykezelőjével eredményesen vehetjük fel a harcot a nem kívánt ActiveX vezérlők ellen.

Az Internet Explorer egy úgynevezett *információs sávval* is gazdagodott, amely az eddigieknél részletesebb adatokkal szolgál a böngészés során bekövetkező eseményekről (például itt jelenik meg az üzenet az előugró ablakok blokkolásáról).

Okosabb lett az *Outlook Express* levelezőprogram is. Folyamatosan figyeli a levelezésünket, és ha vírusgyanús mellékletet talál valamelyik e-mail üzenetben, intézkedik. A levelezőprogram új *Mellékletkezelője* megnyitáskor karanténba helyezi a veszélyes mellékletet, és megakadályozza ezzel annak megnyitását.



A Outlook Express a melléklet megnyitása előtt még egyszer figyelmeztet a veszélyekre

Jó tudni

A szervizcsomag ingyenes letöltéséhez és telepítéséhez keresse fel a **www.microsoft.com/hun/protect** webhelyet, vagy helyezze be a meghajtóba CD/DVD-mellékletünket, és indítsa el a rajta található telepítőállományt.

Automatikus frissítés

A Biztonsági központból az *Automatikus frissítést* is jobban kézben tarthatjuk. A Windows jól ismert automatikus frissítési szolgáltatása rendszeresen ellenőrzi a védelmi rendszer állapotát, és gondoskodik a legújabb frissítések automatikus letöltéséről és telepítéséről. A szolgáltatást a Windows biztonsági központban aktiválhatjuk, ahol azt is megadhatjuk, hogy milyen időközönként (például a hét mely napján, hány órakor) keressen új frissítéseket a rendszer.

Megjegyzés

Sokan emlékezhetnek rá, hogy 2003 augusztusában megjelent a Microsoft Windows XP *1. szervizcsomagja*. Ha valaki akkor, illetve azóta sem telepítette az 1. szervizcsomagot, nem kell aggódnia: az 1. szervizcsomagban szereplő valamennyi frissítés és javítás a 2. szervizcsomagban is megtalálható.

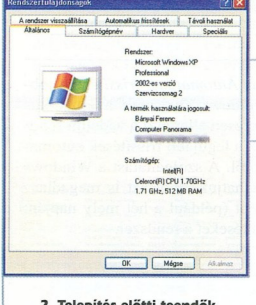
Az XP SP2 telepítése

A Windows XP 2. szervizcsomagját a *Windows XP Home Edition* vagy a *Windows XP Professional* operációs rendszerrel működő számítógépekre egyaránt telepíthetjük. Ha számítógépünket nemrég vásároltuk, az is elképzelhető, hogy a szervizcsomag már telepítve van rá. Régebbi gépen is telepítve lehet már a csomag, ha az *Automatikus frissítés* funkciót bekapcsoltuk rajta. Mielőtt tehát bármihez hozzákezdenénk, ellenőrizzük, hogy a számítógépünkön már telepítve van-e a Windows XP 2. szervizcsomagja.

1. Rendszerellenőrzés

Kattintsunk a jobb gombbal a *Sajátgép* ikonra a munkaasztalon. A felbukkanó menüben válasszuk a *Tulajdonságokat.*

Megjelenik a *Rendszertulajdonságok* ablak. Itt lapozzunk az *Általános* fülre, és ellenőrizzük a *Rendszer* felirat alatt megjelenő információkat. Ha itt a *Szervizcsomag 2* szöveg olvasható, akkor a gépen már telepítve van az XP SP2. Ha a *Szervizcsomag 1* felirat látható, vagy a hely üres, telepíteni kell a Windows XP 2. szervizcsomagját. Az ablak bezárásához kattintsunk a *Mégse* gombra.



A Rendszertulajdonságok alatt megnézhetjük, hogy szükség van-e a szervizcsomag telepítésére

2. Telepítés előtti teendők

A 2. szervizcsomag telepítése előtt néhány lépés megtételére feltétlenül szükség van a biztonság érdekében. Legelőször is készítsünk biztonsági másolatot a fájljainkról. Erről bővebben a Windows XP *Súgó és támogatási* központjában, a *Biztonsági másolatok készítése fájlokról és mappákról* témakörben olvashatunk bővebben.

Ideiglenesen kapcsoljuk ki vagy távolítsuk el a szoftveres tűzfalat és a vírusirtó szoftverünket a telepítés előtt. Sokak ütköznek problémába a telepítés során, mert elfeledkeznek erről. Sok keserűséget, felesleges gondot okozhat, ha ezt nem tesszük meg – többet, mint azt sok tapasztalt PC-felhasználó képzeli. Miután a telepítés befejeződött, kapcsoljuk vissza biztonsági szoftvereinket.

Ellenőrizzük a merevlemezünket a lemezhibák szempontjából. Az XP-ben ez a *chkdsk /f* parancssori futtatását jelenti (*Start/Futtatás*). A művelet végrehajtásához újra kell indítanunk a gépet.

3. Rendszer-visszaállítási pont létrehozása

Az SP2 telepítése előtt hozzunk létre egy rendszer-visszaállítási pontot. Ez egy Windows XP-be épített helyreállító szisztéma, amely automatikusan, naponta „pillanatfelvételeket" készít a Windows rendszerfájljairól, így később visszaállíthatunk egy olyan korábbi állapotot, amikor még minden rendben működött. Igaz, hogy általában az automatikusan mentett visszaállítási pontra is támaszkodhatunk (feltéve, hogy ez a funkció be van kapcsolva), mégis sokkal praktikusabb, ha mi magunk hozunk létre egy-egy ilyen mentést,

Jogtiszta vagy nem jogtiszta?

A Windows XP telepítésekor be kell gépelni egy 25 jegyű sériaszámot, amelyből azután a Windows előállítja a termékazonosító kódot. (Ez a kód a *Rendszertulajdonságok* alatt tekinthető meg.) A Windows XP első szervizcsomagja megvizsgálja ezt a kódot, és ha illegális Windows-másolatot talál, nem hajlandó települni. Hasonló élményben lehet részünk a 2. szervizcsomag telepítésekor is: ha a kód „lopott", a javítócsomag nem telepíthető. A helyzet persze nem ennyire súlyos: a Microsoft nagyvonalúságának köszönhetően csak néhány különösen gyakori termékazonosító kód került fekete listára. Ezek a következők:

XXXXX-640-0000356-23XXX

XXXXX-640-2001765-23XXX

Ha tehát valaki ilyet talál a gépén, ne csodálkozzék, ha a telepítés nem hoz számára sikerélményt. Amúgy a 2. szervizcsomag minden további nélkül a „lopott" Windows XP-kre is telepíthető.

amelyet azután úgy nevezünk el (például *SP2 telepítése előtt*), hogy később könnyedén azonosítani tudjuk. Így szükség esetén egyértelmű lesz, melyik mentési pontot kell használnunk.

Rendszer-visszaállítási pont létrehozásához zárjunk be minden felesleges alkalmazást, majd nyissuk meg a *Rendszer-visszaállítás varázslót:* kattintsunk a *Start* menü *Súgó és támogatás* parancsára.

Ezután válasszuk a *Teljesítmény és karbantartást,* majd a *Módosítások visszavonása a rendszer-visszaállítási szolgáltatással* opciót, végül pedig *A Rendszer-visszaállítás varázsló használata* elemet. Itt válasszuk a *Visszaállítási pont létrehozása* opciót, és adjunk a pontnak egy könnyen azonosítható nevet.

A rendszer-visszaállítási pontnak olyan nevet adjunk, amely később könnyen azonosítható állapotra mutat

Letöltés és telepítés

Ha végeztünk a biztonsági mentéssel, hozzákezdhetünk az XP SP2 csomag telepítéséhez. A csomagot megtalálják CD/DVD-mellékletünkön, vagy letölthetik a **www.microsoft.com/hun/protect** címről is. A fájl mérete hozzávetőleg 270 Mbájt, így aki modemen keresztül kapcsolódik a világhálóra, ne számítson gyors eredményre. ADSL vagy más széles sávú kapcsolaton keresztül a letöltés legfeljebb 1-2 órát vesz igénybe.

Ha mégis a letöltés mellett döntünk, három lépésen kell átverekednünk magunkat.

1. Az SP2 letöltése

Látogassunk el az előbb említett weboldalra (**www.microsoft.com/hun/protect**).

Három lépés távolsága vagyunk a biztonsági frissítéstől

Az *Először:* legördülő menüben jelöljük ki a *Windows XP* elemet, és kattintsunk a *Tovább* gombra.

Kattintsunk a *Windows XP 2. szervizcsomagjának letöltése (ajánlott)* lehetőségre. Megjelenik a *Microsoft Windows Update* webhely.

A Windows Update webhely a Windows internetes bővítménye, amelynek segítségével naprakészen tarthatjuk számítógépünket. A webhelyet rendszeresen bővítik új tartalommal, így a számítógép védelme és gördülékeny működése érdekében mindig beszerezhetjük a legújabb frissítéseket és javításokat.

Az *Üdvözöljük!* képernyőn kattintsunk a *Gyorstelepítés (ajánlott)* lehetőségre. Miután a Gyorstelepítés hivatkozásra kattintottunk, a Windows Update ellenőrzi a rendszerünket, hogy meghatározza, milyen frissítésekre van szüksége.

Ezt követően kattintsunk a *Telepítés* gombra. A letöltés elkezdődik. A kapcsolat sebességétől függően a letöltés rövidebb-hosszabb időt vehet igénybe. Nem kell figyelemmel kísérni a letöltési folyamatot, továbbra is használhatjuk a számítógépet.

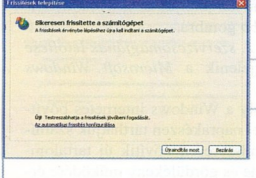
A letöltési folyamat befejeztével megjelenik a Windows XP 2. szervizcsomagjának *Végfelhasználói licencszerződése.*

2. Telepítés a telepítővarázslóval

Elindul a 2. szervizcsomag telepítővarázslója. Kattintsunk a *Tovább* gombra.

Indul a 2. szervizcsomag telepítővarázslója

A telepítési folyamat elkészültével kattintsunk az *Újraindítás most* gombra, hogy a telepítést befejezzük.



A telepítés sikeresen befejeződött

A telepítés után elsőként megjelenő ablak arra kér, hogy kapcsoljuk be az *Automatikus frissítések* szolgáltatást, ha azonban az Automatikus frissítések szolgáltatás beállítása jelenleg *A számítógéphez ajánlott frissítések automatikus letöltése és telepítése,* nem jelenik meg ez a képernyő.

3. Automatikus frissítések bekapcsolása

Az Automatikus frissítések bekapcsolása a legegyszerűbb módja a számítógép védelmének a különféle biztonsági fenyegetések ellen. Ekkor nem kell rendszeresen ellenőriznünk a Windows Update webhelyet, hogy manuálisan letöltsük és telepítsük a legújabb frissítéseket. Az Automatikus frissítések szolgáltatás mindezt helyettünk is elvégzi.

Az Automatikus frissítések bekapcsolásához kattintsunk *A számítógép védelme az automatikus frissítési szolgáltatás azonnali bekapcsolásával (ajánlott)* lehetőségre, majd a *Tovább* gombra.

A 2. szervizcsomag telepítése ezzel befejeződött.

A Biztonsági központ használata

A Microsoft Windows XP 2. szervizcsomagjának telepítése után számos új és továbbfejlesztett szolgáltatás jelenik meg, ezek főbb elemeivel nagy vonalakban már megismerkedtünk. Nézzük most meg őket kicsit közelebbről is.

1. Biztonsági központ megnyitása

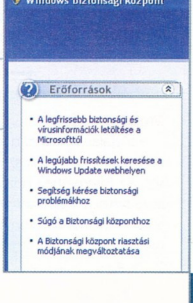
A *Windows biztonsági központ* a számítógép pillanatnyi biztonsági állapotát jelzi, továbbá megjeleníti a számítógép biztonságosabbá tételével kapcsolatos esetleges teendőket is.

A Windows biztonsági központ megnyitásához válasszuk a *Start* menü *Vezérlőpult* parancsát.

A Vezérlőpulton kattintsunk duplán a *Biztonsági központ* elemre.

A Windows biztonsági központ a három alapvető biztonsági szolgáltatás állapotát jeleníti meg, a *Windows tűzfal,* az *Automatikus frissítések* és a *Vírusvédelem* állapotát. Folyamatosan felderíti az esetleges problémákat, és értesítést küld, ha valami figyelmet igényel.

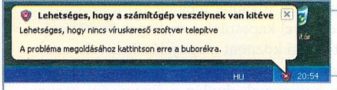
A Biztonsági központban továbbá gyorsan információhoz juthatunk a legújabb vírusokkal és a biztonsági fenyegetésekkel kapcsolatban is, és a biztonsági problémák esetén a Microsoft ügyfélszolgálatának a segítségét is igénybe vehetjük. Bővebb információért csak kattintsunk az *Erőforrások* csoportban levő címsorok egyikére. Itt olyan lehetőségek állnak rendelkezésünkre, mint *A legfrissebb biztonsági és vírusinformációk letöltése a Microsofttól, A legújabb frissítések*



A Biztonsági központ további erőforrásokkal is a felhasználó segítségére siet

keresése Windows Update webhelyen, a *Segítség kérése biztonsági problémákhoz,* a *Súgó a Biztonsági központhoz* és *A Biztonsági központ riasztási módjának megváltoztatása.*

Amennyiben egy vörös pajzs, illetve a *Lehetséges, hogy a számítógép veszélynek van kitéve* üzenet jelenik meg az értesítési területen (a képernyő jobb alsó sarkában), a Windows biztonsági központ ezzel figyelmeztet, hogy törődést igénylő biztonsági probléma adódott.



A Biztonsági központ figyelmeztetése

A figyelmeztetésre kattintva megnyílik a Windows Biztonsági központ, így megtekinthetjük és módosíthatjuk az aktuális biztonsági beállításokat.

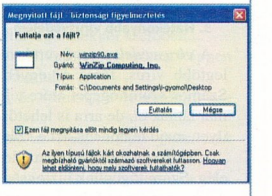
2. A tűzfal konfigurálása

A tűzfal blokkolja az internetes programok hozzáférését a számítógéphez az internetkapcsolaton keresztül. Ha a tűzfal nincs bekapcsolva, előfordulhat, hogy a hackerek hozzáférnek a számítógéphez, és arra olyan kártékony kódot telepítenek, amely megsemmisítheti a fájlokat, vagy a rendszer hibás működéséhez vezet.

Tűzfalat általában mindenhol ajánlatos használni, az internetkapcsolat típusától függetlenül, legyen az telefonos, ISDN- vagy kábelmodem, illetve digitális előfizetői vonal (DSL vagy ADSL).

A 2. szervizcsomag telepítése után, ha olyan programot futtatunk, amely megpróbál az internethez kapcsolódni, előfordulhat, hogy biztonsági figyelmeztetést kapuk a Windowstól. A riasztás közli, hogy a futtatott program megkísérel hozzáférni az internethez, és a Windows tűzfal blokkolta a próbálkozást.

A „gyanús" programok futtatásakor biztonsági figyelmeztetést kapunk



Ekkor három lehetőség közül választhatunk:

Ha a *Tiltás feloldása* gombra kattintunk, a programot felvesszük a Windows tűzfal *kivétellistájára,* így a program ekkor és a jövőben is hozzáférhet az internethez.

Ha a *Tiltás fenntartása* gombra kattintunk, a Windows tűzfal a későbbiekben is blokkolja a programot, így e program esetén többé nem jelenik meg a Windows biztonsági riasztás párbeszédpanel.

Ha a *Rákérdezés később* gombra kattintunk, a Windows tűzfal a későbbiekben is blokkolja a programot, és amennyiben a program kapcsolatot szeretne létesíteni, megjelenik a Windows biztonsági riasztás párbeszédpanel.

A Windows tűzfal beállításait a következőképpen ellenőrizhetjük és módosíthatjuk:

Kattintsunk a *Start* gombra, és válasszuk a *Vezérlőpult* parancsot.

A kivétellistán szereplő programok akadálytalanul kapcsolódhatnak az internethez

Megjegyzés

A tűzfalas védelem nem kívánt velejárója, hogy a számítógépen futó programok számára is megtilthatja az internet elérését. Az internethez hozzáférni próbáló népszerű alkalmazások közé tartoznak az interneten át játszható és a többrésztvevős játékok, valamint bizonyos azonnali üzenetküldésre alkalmas programok.

A Vezérlőpulton kattintsunk a *Biztonsági központ* elemre.

A Biztonsági központ ablakának alsó részén kattintsunk a *Windows tűzfal* elemre.

3. Hatékonyabb vírusvédelem

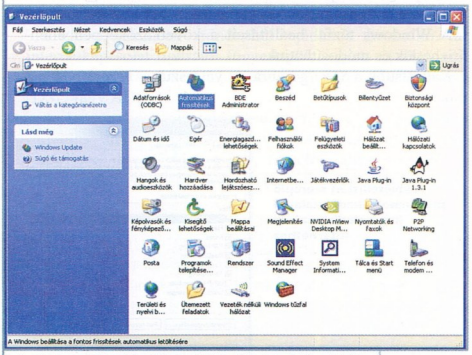
A *vírusvédelmi* szoftverek megvédik a számítógépünket a legtöbb vírus, féreg és egyéb biztonsági fenyegetés ellen. Számos számítógépet előre telepített vírusvédelmi programmal látnak el, de arra is lehetősége van, hogy mi vásároljunk ilyet, majd telepítsük azt a számítógépünkre.

A vírusvédelmi program telepítése sajnos önmagában nem elég. Számítógépünk biztonságának megőrzéséhez a vírusvédelmi programot folyamatosan frissíteni kell.

A *Windows biztonsági központ* felismeri a nagyobb gyártók által készített vírusvédelmi programokat. Biztonsági figyelmeztetés jelenik meg, ha a Windows nem talál telepített vírusvédelmi programot a számítógépen, vagy ha a felismert program nem naprakész.

4. Automatikus frissítések

Az *Automatikus frissítések* szolgáltatás 2. szervizcsomagban található fejlesztései révén könnyen kiválaszthatjuk, mikor szeretnénk a legújabb frissítéseket letölteni és telepíteni,



Az Automatikus frissítés beállításait a Vezérlőpultból is elérhetjük

továbbá a telefonos kapcsolattal rendelkező felhasználók új technológiához jutnak a frissítések hatékonyabb letöltése érdekében. Ha még nem kapcsoltuk be az Automatikus frissítések szolgáltatást, a számítógépünk jóval sérülékenyebb a vírusokkal és egyéb biztonsági fenyegetésekkel szemben.

Az Automatikus frissítések beállításait a következőképpen ellenőrizhetjük, illetve módosíthatjuk:

Kattintsunk a *Start* gombra, és válassza a *Vezérlőpult* parancsot.

A Vezérlőpulton kattintsunk az *Automatikus frissítések* elemre.

Ha az Automatikus frissítések szolgáltatás bekapcsolt állapotban van, a Windows XP rendszeresen ellenőrzi a *Windows Update* webhelyet a letölthető legújabb frissítésekkel kapcsolatban, és automatikusan le is tölti azokat. Ezt követően a frissítések telepítésére vonatkozó figyelmeztetést jelenít meg az értesítési területen.

A frissítéseket ugyanis letöltésük után telepíteni kell a számítógépre, hogy érvénybe lépjenek. Az alapértelmezés szerinti beállítás *(Minden nap, 3:00)* azt jelenti, hogy az Automatikus frissítések szolgáltatás által letöltött frissítések valójában ebben az időpontban települnek a számítógépre, de a felhasználó ettől eltérő ütemezést is beállíthat.

A Windows az általunk megadott időpontokban automatikusan letölti a biztonsági frissítéseket

5. Biztonságosabb levelezés

Számos vírust és férget e-mail üzeneteken keresztül küldenek. Bármilyen e-mail üzenet tartalmazhat a számítógépre vagy az azon tárolt adatokra nézve veszélyes vírust, még a látszólag ártalmatlan üzenetek is. A 2. szervizcsomag részét

képező új mellékletkezelő alapértelmezés szerint csak a lehetséges veszélyforrásként számon tartott fájltípusok mellékletként való megnyitását tiltja le.

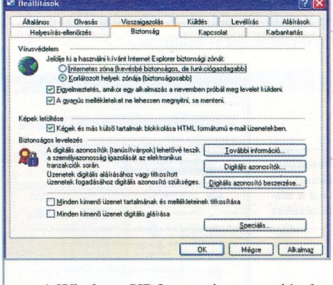
A Windows XP 2. szervizcsomagjának telepítését követően az *Outlook Express* programhoz tartozó alapértelmezett beállítások meggátolják az interneten keresztüli jogosulatlan hozzáférést a személyes adatainkhoz.

Az Outlook Express programban egyszerűen az egyéni igényekhez igazíthatók az elektronikus levelezés biztonsági beállításai. Az alapértelmezett beállítások megváltoztatásával azonban számítógépünk sebezhetőbbé válhat.

Az Outlook Express beérkezett e-mail üzenetekkel kapcsolatos biztonsági beállításait a következőképpen érhetjük el.

Nyissuk meg az Outlook Express programot. Válasszuk az *Eszközök* menü *Beállítások* parancsát, majd lépjünk a *Biztonság* panellapra.

A Microsoft javasolja az alapértelmezett beállítások megőrzését a számítógép és a személyes adatok védelme érdekében.



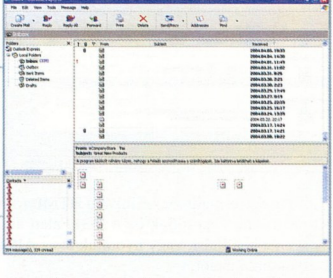
Az Outlook Express alapbeállításai kielégítő biztonságot nyújtanak a veszélyes küldemények ellen

A Windows XP 2. szervizcsomagjának egyik újításaként az Outlook Express hatékonyabban segít a levélszemét mennyiségének csökkentésében, mert megakadályozza a rosszindulatú levélküldők számára az e-mail címünk megszerzését. A kéretlen üzenetek és a szemétlevelek például gyakran olyan képeket tartalmaznak, amelyek a küldő számítógépéről történő letöltés után jelennek meg. A képek letöltődésekor az üzenet küldője értesítést kap, és így megtudja, hogy az e-mail címünk valóban létezik és használatban van, tehát további kéretlen küldemények potenciális célpontjának tekinthető. A spamküldők gyakran láthatatlan, egy pixel méretű képekbe linkeket építenek be. Ezeket a tartalommal együtt letöltjük, és így meg tudják állapítani, hogy az e-mail fiókunk még aktív-e. Ha egy e-mail ilyen képeket tartalmaz, azonnal figyelmeztetés jelenik meg a képek blokkolásáról. Ha vannak olyan objektumok, amelyeket látni szeretnénk, ezeket az e-mail fejlécében rendelkezésre álló mezőre kattintva utólag betölthetjük.

Alapértelmezés szerint az Outlook Express levélszemét elleni eljárása csak engedélyezésünket követően teszi lehetővé a külső forrásból származó képek és ábrák letöltését. Célszerű minden fogadott képet letiltani a megbízható forrásból származók kivételével.

A megbízható forrásból származó e-mail üzenetben szereplő képeket a következőképpen tekinthetjük meg.

Indítsuk el az Outlook Express programot, és nyissuk meg az adott e-mail üzenetet.



Az Outlook Express blokkolhatja a megbízhatatlan forrásból származó üzenetekben érkező képeket

Ha az üzenet letiltott képeket tartalmaz, ezt a következő üzenet jelzi: *A program blokkolt néhány képet, nehogy a feladó azonosíthassa a számítógépet. Ide kattintva letöltheti a képeket.*

Kattintsunk az üzenetsávra. A képek betöltődnek és megtekinthetjük őket.

Tipp

Ha a képeket továbbra is azonnal szeretnénk betöltetni, az *Eszközök/Beállítások* alatt, a *Biztonság* fülnél oldjuk fel a Képek és más külső tartalmak blokkolása... beállítást, ami azonban a már ismert kockázatokat rejti magában.

A szervizcsomag telepítését követően az e-maileket nem HTML, hanem egyszerű szöveges formátumban is megjeleníthetjük. Így a szkriptek, amelyek eddig automatikusan lefuttottak, egyáltalán nem aktiválódnak.

Menjünk az *Eszközök* alatt a *Beállításokra*, majd válasszuk az *Olvasás* fület, és tegyünk pipát az *Összes üzenet egyszerű szöveg formátumban történő olvasása* elé.

Biztonságosabb, ha az e-maileket szöveges formátumban jelenítjük meg

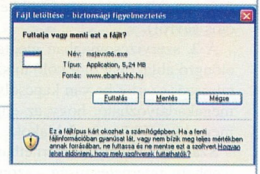
Ha egy e-mailt mégis inkább HTML formátumban akarunk megnézni, kapcsoljuk be a *Nézet* alatt az *HTML formátumú üzenet* beállítást, vagy nyomjuk le az **Alt + Shift + H** billentyűkombinációt.

6. Előugró ablakok blokkolása

A 2. szervizcsomagban az *Internet Explorerhez* tartozó frissítések és kiegészítések között olyan alapértelmezés szerinti biztonsági beállítások szerepelnek, amelyek segítenek a lehetséges biztonsági fenyegetések azonosításában, és figyelmeztetnek velük kapcsolatban.

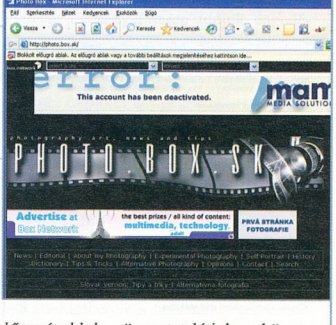
Ha olyan helyre kattintunk, amely letöltést indít el, biztonsági figyelmeztetés jelenik meg. Ekkor kiválaszthatjuk, hogy a letöltést folytatjuk-e vagy elutasítjuk.

Fájl letöltésekor mindig biztonsági figyelmeztetést kapunk



Az Internet Explorer *információs sávja* segítségével könnyebben tudomást szerezhetünk az internet böngészése közben előforduló problémákról. Az információs sáv csak szükség esetén jelenik meg, hogy figyelmeztessen a biztonsági kockázatokkal kapcsolatban – még azok bekövetkezte előtt –, így eldönthetjük, továbblépünk-e vagy sem. Ezenkívül értesít az előugró ablakok blokkolásakor is, és lehetőséget ad azok megtekintésére. A választási lehetőségeket tartalmazó legördülő menü megnyitásához kattintsunk az Internet Explorer információs sávjára.

Az Internet Explorer információs sávjában értesülhetünk az előugró ablakok blokkolásáról



Ha a *Blokkolt előugró ablak...* üzenetet látjuk, a következő lehetőségek közül választhatunk: *Előugró ablakok ideiglenes engedélyezése* (megtekinthetjük az adott előugró ablakot), *Webhely előugró ablakainak állandó engedélyezése* (az adott webhelyen levő előugró ablakok mindig megjelenhetnek), *Beállítások* (további lehetőségekért megnyitja az Előugró ablakok blokkolása párbeszédpanelt) és

Információs sáv — súgó (többet megtudhatunk az információs sávról).

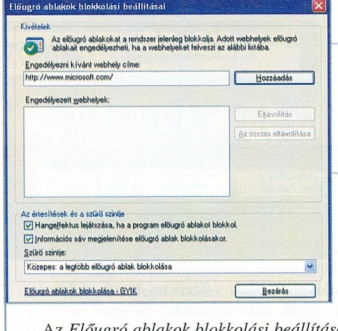
A 2. szervizcsomagban megtalálható az Internet Explorer előugró ablakokat blokkoló új szolgáltatása is, amely alapértelmezés szerint be van kapcsolva. Ezentúl a legtöbb esetben megakadályozható, hogy az engedélyünk nélkül jelenjenek meg előugró böngészőablakok.

Számos webhely – internetbank, kormányzati információs webhely, internetes újság – azonban gyakran használ előugró ablakokat az információk megjelenítéséhez. Ha rendszeresen látogatunk előugró ablakokat tartalmazó webhelyekre, felvehetjük őket a *kivétellistára.* Így ha bármikor felkeressük az adott webhelyet, az előugró ablakok akadály nélkül megjelennek.

Webhelyet a következőképpen vehetünk fel az Internet Explorer előugró ablakokat blokkoló szolgáltatásának kivétellistájára.

Nyissuk meg az Internet Explorer böngészőt.

Kattintsunk az *Eszközök* menü *Előugró ablakok blokkolása* parancsára, majd az *Előugró ablakok blokkolási beállításai* menüpontra.



A kivétellistára felvett webhelyek akadálytalanul megjeleníthetnek előugró ablakokat

Az *Előugró ablakok blokkolási beállításai* párbeszédpanelen az *Engedélyezni kívánt webhely címe* mezőbe írjuk be a webhely teljes címét (például: **http://www.microsoft.com**).

Kattintsunk a *Hozzáadás,* majd a *Bezárás* gombra.

Tipp

Tegyünk a *Beállítások* alatt pipát a *Hangeffektus lejátszása* elé. Így minden blokkolt ablakról hangjelzést kapunk, és nem maradunk le az esetleg fontos információkról a weboldalakon. Egy kattintással a popup-ikonra jobbra lent az Internet Explorerben eljutunk az *Előugró ablakok kezeléséhez,* ahol engedélyezni vagy tiltani tudjuk a popupokat.

7. Bővítmények kezelése

A 2. szervizcsomagban található másik új funkcióval letilthatjuk az Internet Explorer *bővítményeit* (általában az *ActiveX-vezérlőket*). Sok program – kérve vagy kéretlenül – betelepül az *Internet Explorerbe.* Ezek közé tartozik például a *Windows Messenger,* az *ICQ,* a *Google* eszközsor vagy a *Macromedia Flash.*

Spyware-ek, mint például az *Alexa* plugin is, észrevétlenül a böngészőre akaszkodhatnak. Az Internet Explorer javított bővítménykezelőjével teljes áttekintést kapunk ezekről a diszkréten megbúvó programokról. A bővítménykezelő segítségével a plugineket az Internet Explorerben egyetlen kattintással, nagyon gyorsan és kényelmesen tudjuk engedélyezni vagy letiltani.

A bővítményeket a következőképpen tilthatjuk le az Internet Explorer *bővítménykezelőjével:*

Nyissuk meg az Internet Explorer böngészőt.

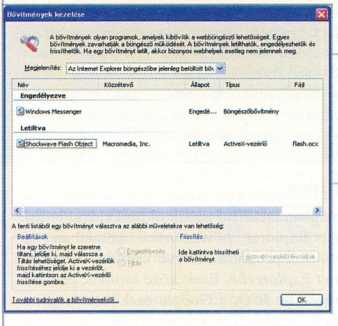
Kattintsunk az *Eszközök* menü *Bővítmények kezelése* parancsára.

A *Bővítmények kezelése* párbeszédpanelen az *Engedélyezve* felirat alatt kattintsunk a kívánt bővítményre.

A *Beállítások* területen kattintson a *Tiltás,* majd az *OK* gombra.

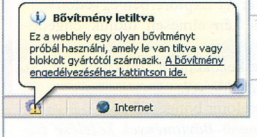
A bővítményeket kétféleképpen jeleníthetjük meg: a Megjelenítés melletti mezőben kiválaszthatjuk például *Az Internet Explorer böngészőbe jelenleg betöltött bővítmények* bejegyzést, de jobban áttekinthetjük a helyzetet, ha a másik lehetőséget, *Az Internet Explorer által használt bővítményeket* választjuk. Ha egy *ActiveX*-modult találunk, frissíthetjük a szóban forgó elemet, mégpedig az *ActiveX-vezérlő frissítése* gombra kattintva.

Az Internet Explorer figyelmeztetést jelenít meg az értesítési területen, ha olyan webhelyre látogatunk, amelyhez a letiltott bővítmények egyike szükséges. A figyelmeztetésben



Az Internet Explorer bővítménykezelőjével engedélyezhetünk vagy letilthatunk bővítményeket

szereplő hivatkozás az Internet Explorer bővítménykezelőjére mutat, így könnyen engedélyezhetjük a szükséges bővítményt.



Az Internet Explorer figyelmeztet, ha letiltott bővítménybe botlunk

Tipp

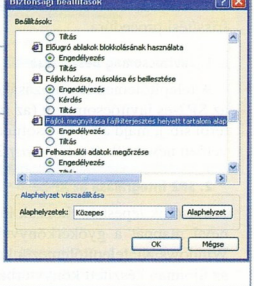
Először kapcsoljunk ki minden bővítményt, amelyet nem tudunk egyértelműen azonosítani, és csak igény esetén kapcsoljuk őket vissza. Így javítunk a biztonságon és erőforrást takarítunk meg.

8. Biztonságos böngészés

Több mint 90 százalékos piaci részesedésével az *Internet Explorer* a legelterjedtebb webböngésző, és mint ilyen, a hackertámadások kedvelt célpontja. Nyissuk meg a biztonsági beállításokat az *Eszközök* menü *Internetbeállítások* pontja alatt, a *Biztonság* fülre kattintva.

A *Zóna biztonsági szintje* alatt, az *Egyéni szint* gombra kattintva új biztonsági beállításokat érhetünk el. Ezek között szerepel például a *Fájlok megnyitása fájlkiterjesztés helyett tartalom alapján*. Ez hivatott leleplezni például azt, ha egy trójai kártevő képnek álcázza magát. Az intranet-biztonság kapcsán további lépést jelent a helyes irányba az a lehetőség, hogy a helyi hálózathoz biztonsági zónát lehet konfigurálni. Így sok hackertámadást eleve kizárhatunk.

A biztonságosabb internetezést szolgálják a rendelkezésre álló tartalomzónák, illetve biztonsági szintek



A fájlokat kiterjesztésük alapján is megnyithatjuk – biztonsági okokból

Tipp

Kattintsunk a *Biztonság* fülnél az *Egyéni szintre*, és válasszuk ki a *közepeset*. Itt a biztonsági óvintézkedések megfelelően szigorúak.

9. Futtatásvédelem

A 2. szervizcsomaggal a Windows XP *futtatásvédelmet* is kap *(Execution Protection)*. Ez alapvetően megakadályozza a programkódok indítását. Ehhez a teljes memóriát *NX-Flaggel* (NX=„No execute") jelöli meg. Csak ha a Windows maga ír kódot a memóriába, állítja az NX-Flaget inaktívra. Ez azt jelenti, hogy ha egy hacker megkísérel egy puffertúlcsordulással operáló kóddal olyan területekre írni, amelyek nincsenek engedélyezve, a kód egyszerűen nem lesz futtatva – a támadás alól ez kihúzza a talajt. Azonban a processzornak támogatnia kell az Execution Protectiont. Az *AMD* az *Athlon 64*-gyel elöl jár, az *Intel* kilátásba helyezte a lemaradás pótlását. A probléma mindezzel csak az, hogy azok a programok, amelyek nem tartják magukat a programkód és az adatok szétválasztásához, lefagynak.

SP2 az XP telepítőlemezén

Az SP2-t úgy is beágyazhatjuk az XP operációs rendszerbe, hogy létrehozunk egy új, SP2-vel kiegészített XP telepítőlemezt. Így a javítások már a telepítéskor ott vannak a rendszerben, s feleslegessé válik a későbbi hosszadalmas frissítési procedúra.

1. Javítócsomag beszerzése

A telepítőlemez létrehozásához legelőször is szerezzük be az SP2-es javítócsomagot (az internetről, a lap CD-mellékletéről stb.), majd a fájlt másoljuk be a *c:\sp2* mappába. Ezt követően nevezzük át a fájlt *xpsp2.exe*-re.

2. SP2 integrálása az XP-be

Második lépésként hozzuk létre a merevlemezünkön az *xp* nevű mappát a gyökérkönyvtárban *(c:\xp)*, majd fogjuk a Windows XP telepítőlemezünket, és másoljuk a CD tartalmát az újonnan készített könyvtárba.

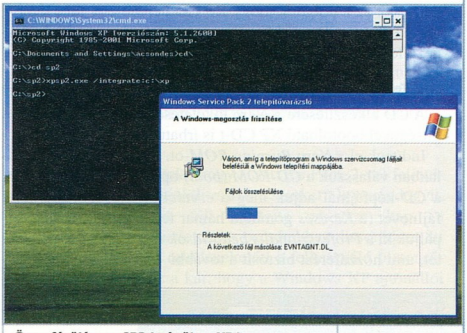
Nyissuk meg a parancssort a *cmd* paranccsal *(Start/Futtatás/cmd)*. A parancssorban gépeljük be a következőt (mindegyik sor után leütve az *Enter*t):

```
cd\
cd sp2
xpsp2.exe /integrate:c\xp
```

Ekkor megindul az *integrálás* folyamata. Először megtörténik a fájlok kicsomagolása az xpsp2.exe-ből.

Az integrálás első mozzanata a fájlok kibontása

Ezután végbemegy az SP2 beépülése az alap XP-be. A művelet végén egy kis ablak tájékoztat arról, hogy az integrált telepítés sikeresen befejeződött.

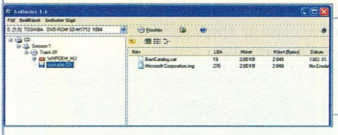


Összefésülés: az SP2 beépül az XP-be

3. Lemez bootolhatóvá tétele

A következő lépés a lemez bootolhatóvá tétele. Ehhez szükségünk van egy fájlra az XP lemezről. Ennek kimásolásához szükségünk lesz az *ISOBuster* nevezetű programra **(www.smart-projects.net/isobuster/).** Töltsük le, majd telepítsük, végül indítsuk el az ISOBustert. A kezelőfelület nyelvének a magyart is beállíthatjuk.

Amikor berakjuk az XP CD-t, válasszuk a bal oldalon található *Bootable CD* pontot. Ekkor a jobb oldalon feltűnik egy fájl a *Microsoft Corporation.img* névvel (vagy valami-



ISOBuster: a bal oldali panelen válasszuk a Bootable CD pontot

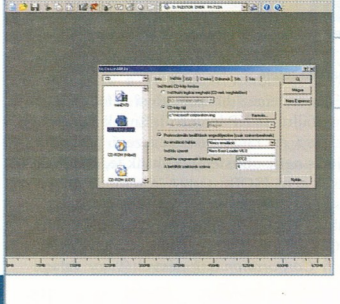
lyen más elnevezéssel – a lényeg, hogy *.img* kiterjesztésű legyen). Ezt a piciny állományt kell kicsomagolnunk, méghozzá úgy, hogy a jobb gombbal rákattintunk, majd a *kifejt • extract* parancsot választjuk. Ezt másoljuk a *c:* gyökérkönyvtárába, majd zárjuk be az ISOBustert.

Ezután jegyezzük fel az XP CD-nk nevét – a *Sajátgépnél* vessünk rá egy pillantást. Ez lehet például *WXPOEM_HU*, de ettől eltérő is a különböző XP változatok esetében. Most már csak az a dolgunk, hogy XP CD helyett egy üres lemezt helyezzünk a CD-írónkba, és már kezdetét is veheti a következő lépés, a CD megírása.

4. Telepítő CD megírása

A CD elkészítésére a *Nero* tökéletesen megfelel, mivel segítségével bootolható XP CD-t is írhatunk.

Indítsuk el a *Nero Burning ROM*-ot. Az *Új összeállítás* ablakban válasszuk a *CD-ROM (boot)* opciót. Az *Indítás* fülön, a CD-képfájlnál adjuk meg a *c:\microsoft corporation.img* fájlnevet (a *Keresés* gombbal hamar fellelhetjük). Ezután pipáljuk ki a *Professzionális beállítások engedélyezése* négyzetet, ami hozzáférést biztosít a további – szükséges – beállításokhoz. Az *Emuláció fajtájánál* adjuk meg a *Nincs emulációt,* majd változtassuk *A betöltött szektorok számát* 4-re. A *Szektorszegmensek töltését* feltétlenül hagyjuk a megadott 07C0 értéken.



Nero: az Indítás fülön eszközölt beállítások

Ha ezzel megvagyunk, kattintsunk a *Címke* fülre, ahol adjuk meg az XP CD-nk korábban feljegyzett nevét (a mi esetünkben ez a *WXPOEM_HU* volt). Ha ez is megtörtént, nyomjunk az ablak jobb oldalán található *Új* gombra. Ekkor megjelenik a Nero Burning ROM fő ablaka.

Az ablak jobb oldalán keressünk rá a *c:\xp* mappára. Válasszuk ki az összes ott található fájlt, majd másoljuk az új CD-re. Ezután már csak annyi a feladatunk, hogy rábökjünk az írást aktivizáló gombra. A munka végeztével ne feledkezzünk meg a c:\microsoft corporation.img állomány és a c:\xp, valamint a c:\sp2 mappák törléséről.

Fájlfuttatási védelem

A Windows XP Service Pack 2 az új biztonsági funkciók egész csokrát kínálja. Abszolút biztonság azonban – mint tudjuk – nincsen, így az SP2 is néha-néha foltozásra szorul.

1. Megjelölt fájlok

Vajon tudja-e mindenki, hogy a Service Pack 2-vel feljavított Windows XP megjelöli a letöltéseinket? Így mindegyik potenciális veszélyes fájl egyfajta pecsétet kap, a diszkóbejáratokban osztogatott pecsétekhez hasonlóan. Itt azonban a megjelölés mindenekelőtt a felhasználó biztonságát szolgálja. Csak az a kár, hogy a Windows XP ajtónállói még mindig túl sok nemkívánatos vendéget átengednek, a Windows XP Service Pack 2 biztonsági falán tehát van még néhány rés. Egy ilyen, nem is olyan rég ismertté vált résről olvashatunk az alábbiakban.

2. AES (Attachement Execution Service)

A nem biztonságos „Internet" zónából letöltött fájlok megjelölése mögött az úgynevezett AES (Attachement Execution Service) funkció rejlik. Amennyiben a felhasználó egy letöltött fájlt a *Windows Explorerben* (Intézőben) szeretne elindítani, a Windows egy figyelmeztetést küld, hogy ez a fájl az internetről származik, és ezért potenciális veszélyt rejt magában.

Azonban a Windows csak azokat a letöltéseket és csatolá-

sokat jelöli meg, amelyek az *Internet Explorer*, az *Outlook Express* vagy a *Windows Messenger* programokon keresztül jutottak a merevlemezre. Amennyiben más böngészőt használunk, például a *Mozilla Firefoxot* vagy pedig egy alternatív e-mail programot, például az *Eudorát* vagy a *Thunderbirdöt*, akkor a fájlfuttatási védelem nem lép érvénybe.

A Windows Explorernek az AES-sel összefüggésben egy veszélyes hibája van. Amennyiben egy fájl egy potenciálisan veszélyesként megjelölt fájllal kicserélődik, abból a Windows Explorer először semmit sem észlel. Csupán a Windows újraindítása után frissíti az AES információit. A kicserélt fájl biztonsági visszakérdezés nélkül indítható. Ha valaki szeretne visszaélni ezzel a hibával, annak a kártékony fájlt valamilyen úton-módon egy másik felhasználó számítógépére kell csempésznie, majd arra kell késztetnie, hogy egy ártalmatlan fájlt kicseréljen erre a kártékonyra, végezetül futtassa azt.

3. Potenciálisan veszélyes fájlok

Hogy a Windows egy fájlt potenciálisan veszélyesnek jelölt-e, az könnyen és gyorsan megállapítható. A Windows Intézőben kattintsunk a jobb egérgombbal a fájlra, majd válasszuk ki a felbukkanó menüben a *Tulajdonságok* pontot. A Tulajdonságok ablak *Általános* fülének alsó szélén található a *Biztonság* tartomány, amelyben egy szöveg utal arra, hogy a fájl egy másik számítógépről származik, és ezért a hozzáférés esetleg biztonsági okokból blokkolva van. Amennyiben ugyanazt a fájlt például egy másik böngészővel töltjük le, akkor hiányzik a Biztonság tartomány. A Tiltás feloldása gombra kattintva megszüntethetjük a fájl blokkolását.

A fájltulajdonságok között jó esetben ott találjuk a Biztonságra vonatkozó részt is

Veszélyes üzenetek

A Service Pack 2 Windows tűzfala lényegesen több beállítást kínál, mint a régi *Internet Connection* tűzfal. Segítségével hatékonyan szabályozhatjuk az üzenetküldő szoftverek tevékenységét.

1. Személyi tűzfalvédelem

A személyi tűzfalnak az a dolga, hogy megvédje a számítógépet a veszélyes kapcsolatfelvételektől. A különféle megnyitott portokon keresztül ugyanis a támadók hozzáférhetnek a számítógépünkhöz. Az alapbeállítások szerint a tűzfal éppen az ilyen betörési próbálkozások ellen nyújt védelmet, mégpedig oly módon, hogy blokkolja a számítógép nyitott portjait.

A gépen azonban különféle üzenetküldő alkalmazások is lehetnek, amelyek számára engedélyeznünk kell a külső kapcsolatokat. Ilyen program például a *Windows Messenger* vagy az *ICQ*.

Indítsunk el egy üzenetküldő programot, például az ICQ-t. Legkésőbb a bejelentkezés után közbelép a Windows tűzfal, és biztonsági figyelmeztetést küld. A párbeszédablakban látható három gomb közül a középsőre kattintva engedélyezhetjük a program funkcióinak a korlátozás nélküli használatát. Mostantól az ICQ az internetről bejövő kapcsolatokat anélkül fogadhatja, hogy a Windows tűzfal közbeszólna. Most ellenőrizzük le az előzőleg elvégzett beállításokat a Windows tűzfal felhasználói felületén.

2. A kapcsolóközpont

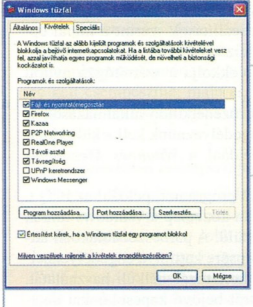
A Windows tűzfal felhasználói felületén rövid áttekintést nyerhetünk a különböző beállítási lehetőségekről.

Ehhez nyissuk meg a *Windows Biztonsági központját* a *Start* menü alatt található *Vezérlőpultból*. Az ablak alsó szélén található *A következő biztonsági beállításainak kezelése* terület alatt válasszuk a *Windows tűzfal* pontot.

A megegyező nevű ablak *Általános* fülén látható, hogy be van kapcsolva a tűzfal. Ezzel megakadályozzuk a kívülről, vagyis a helyi hálózatról vagy az internetről érkező hozzáférési próbálkozásokat a számítógépünkhöz. A párbeszédablak alsó szélén található *Mi egyebet érdemes még tudni a Windows tűzfalról?* hivatkozás alatt, a *Súgó és támogatás* központban újabb rövid összefoglalást nyújt a Microsoft az új

biztonsági eszközről. Ennek elolvasását követően ismét zárjuk be a Súgó és támogatás ablakot.

A Windows tűzfal ablakhoz visszatérve válasszuk a *Kivételek* fület. Itt találhatjuk az olyan programok és szolgáltatások listáját, amelyet a tűzfal már felismert. A programnevek előtti pipa azt jelzi, hogy a program elfogadhatja a kívülről érkező kapcsolódási próbálkozásokat. A nem kipipált alkalmazásokat és az itt még nem szereplő alkalmazásokat blokkolja a tűzfal.



A Kivételek listáján szereplő programok fogadhatják a kívülről érkező kapcsolatokat

Minden esetben ügyeljünk arra, hogy a programlista alatt található *Értesítést kérek, ha a Windows tűzfal egy programot blokkol* beállítás aktiválva legyen. Hiszen megtörténhet, hogy egy szolgáltatást véletlenül blokkolunk a tűzfalon keresztül, és ezért nem működik egy alkalmazás a Windows alatt.

A *Program hozzáadása* gombon keresztül a lista kibővíthető újabb alkalmazásokkal. Ez azonban csak akkor célszerű, ha a számítógépet olyan valaki számára állítjuk be, akinek túl érthetetlenek a tűzfal figyelmeztető jelentései. A tűzfal egyébként úgyis megjelenik akkor, amikor a szóban forgó alkalmazás az első alkalommal jelentkezik.

A *Port hozzáadása* gombon keresztül megnyithatunk egy portot a Windows alatt, méghozzá attól az alkalmazástól függetlenül, amelyik emögött a port mögött rejlik. Ettől a beállítástól azonban jobb, ha távol tartjuk magunkat, mivel egy állandóan nyitva lévő port nagyon veszélyes támadási célpontot képez.

A *Speciális* fülön találhatjuk a számítógépünk összes hálózati kapcsolatát. Alapbeállítás szerint mindegyik rendelkezik egy pipával, és ezért a Windows tűzfal felügyeli őket a beérkező kapcsolatok szempontjából. A *Biztonsági naplózás* és az *ICMP* alatt található beállítások csak a haladók számára érdekesek. Az *Alapértelmezett beállítások* területen található *Alapértelmezett* gombra kattintva a tűzfalon végrehajtott módosítások mindegyikét visszavonjuk. Ezt az utolsó mentőövet abban az esetben használjuk, ha már semmi más nem segít.

3. A fájlmegosztás buktatói

Ha otthon egy kis helyi hálózatot (LAN) üzemeltetünk, akkor a Windows tűzfalban engedélyeznünk kell a *Fájl- és nyomtatómegosztás* beállítást. Ellenkező esetben a hálózat többi felhasználója nem férhet hozzá a saját megosztott mappájához vagy könyvtárához. Éppen itt mutat fel az új XP tűzfal egy nagy rést, amely megtámadhatóvá teszi a saját számítógépet az interneten. Nézzük, hogyan küszöbölhető ki ez a hiba?

A Windows tűzfal biztonsági falán keletkezett résen keresztül az összes olyan számítógép és laptop veszélyben van, amely többféle hálózati csatlakozást használ, például LAN-kapcsolatot hálózati adapterrel, valamint analóg-, ISDN- vagy DSL-modemes kapcsolatot. A számítógép összes csatlakozóját felsorolja a tűzfal a *Speciális* fülön. Figyelem: amennyiben itt nem jelenik meg LAN-kapcsolat, váltsunk át egyszerűen a *Kivételek* fülre, és távolítsuk el a *Fájl- és nyomtatómegosztás* bejegyzés előtt található pipát, majd kattintsunk az *OK* gombra.

Mint a képen is látható, az első helyen az internetes kapcsolat áll, amely az internetes hozzáférést engedélyezi az ISDN adapteren keresztül. A LAN-kapcsolat lehetővé teszi a hozzáférést a helyi hálózathoz egy hálózati kártyán keresztül. A kapcsolatok előtti pipák azt jelzik, hogy a Windows tűzfal az érintett kapcsolat esetében engedélyezett. Példánkban a Windows tűzfal az internetkapcsolatot és a helyi kapcsolatot is felügyeli.

Váltsunk át a *Kivételek* fülre. Itt a blokkolt (pipa nélküli) és az engedélyezett szolgáltatások (kipipált) vannak listázva. A *Fájl- és nyomtatómegosztás* bejegyzés előtt található pipa arról tanúskodik, hogy a Windows tűzfal ezt a szolgáltatást minden olyan hálózati kapcsolat számára engedélyezi, amelyek a *Speciális* fülön ki vannak pipálva. Jelöljük ki a *Fájl- és*