HARMADIK FEJEZET

Az ügyfelek biztonsága

A fejezet tartalma:

Biztonság: általános bevezető

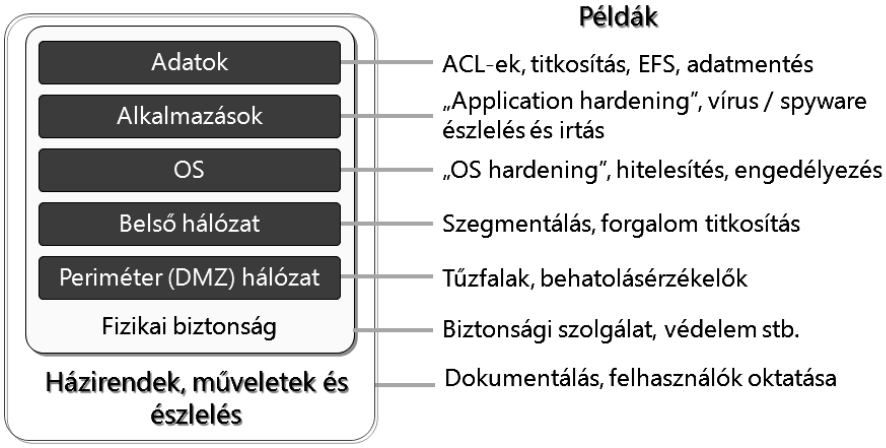
Ellentétben a régmúlttal, ma már sem az önálló számítógépek, sem a számítógép-hálózatok nem tekinthetők zárt rendszernek. A jelenben az informatikai eszközök milliói állnak egymással kölcsönös kapcsolatban (pl. az internet segítségével), illetve a szervezetek hálózatához nem egyszer külső szereplők (pl. szállítók, partnerek, ügyfelek) is hozzáférnek. Ennek következtében jogosulatlan személyek is hozzáférhetnek az e-mailben, kereskedelmi tranzakciókban és a szimpla fájlokban rögzített információkhoz. Mivel az informatika fejlődése és ezzel együtt az állandóan bővülő alkalmazása továbbra is robbanásszerű, a számítógépekre, tárolóeszközökre rengeteg adat és információ kerül, amelyek jelentős része érzékeny és fontos.

Ismerve az emberi természetet, azaz például a kényelem és a biztonság együttes teljesülésének esélyeit, figyelembe véve a fenyegetések fajtáinak fejlődését, valamint a számítógépek közötti kapcsolatok bővülését, a biztonsági visszaélések száma sohasem fog nullára csökkenni. Nagymértékben tompítani tudjuk azonban az illetéktelen felhasználás és számítógépes bűnözők kártékony hatását, ha megfelelő szakértelemmel rendelkezünk, alkalmazzuk a biztonsági alapelveket, és használjuk az elérhető, integrált biztonsági megoldásokat.

Ezek alapján tehát leszögezhetjük: bármilyen számítógépes munkakörnyezetben az egyik legfontosabb alapelv az adatok biztonságos tárolása, az erőforrások felügyelt publikálása valamint az ezekhez történő hozzáférés korlátozása,

illetve felügyelete. Az informatikai infrastruktúra biztonságossá tétele két alapvető célt kell, hogy kitűzzön maga elé: amennyire csak lehet, csökkenteni a külső és belső incidensek számát, valamint növelni az esetlegesen mégis előforduló hibák észlelési arányát. Ha ezt a két területet megfelelően ellenőrzésünk alatt tudjuk tartani, általában biztonságos környezetről beszélhetünk.

Mivel a teljes infrastruktúra is több szintből áll, a biztonsági megoldások is több rétegre bonthatók, így a fizikai biztonságtól (a helyiség őrzése) egészen az adatok képernyőn történő megjelenítéséig számos „kaput” építhetünk fel.



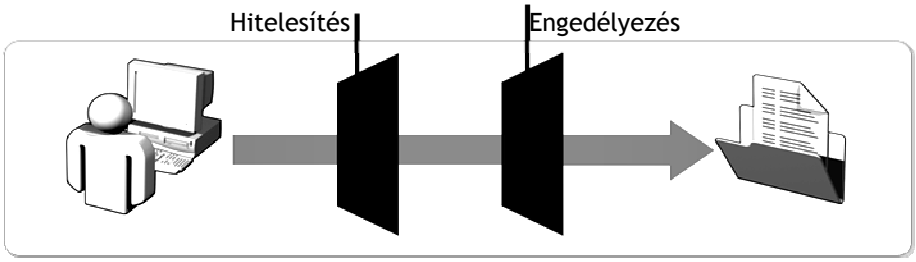
3.1. ábra: *Egy példa a biztonsági szintek általános kialakítására*

Szándékaink szerint ebben a fejezetben, (illetve a könyv más pontjain is) az első három szinttel foglalkozunk részletesen, azaz az adataink, az alkalmazásaink, illetve magának az operációs rendszernek a védelmére vonatkozó elveket és konkrét megoldásokat ismertetjük.

Az erőforrás-kezelés alapjai

A felhasználók (és a számítógépek) hozzáférését az adatokhoz és egyáltalán a rendszer egészéhez úgynevezett hitelesítési (autentikációs) folyamatokkal biztosítjuk. Akár szóló gépről van szó, akár hálózatról, minden felhasználónak célszerűen olyan egyedi azonosítója van, melynek segítségével egyértelműen azonosíthatóvá is válik. A **hitelesítést** – mely során megbizonyosodunk majd a bejelentkező fél identitásáról – az autorizáció, vagyis az **engedélyek megadása** követheti, amely alapja egy előzetes és eltárolt engedély meghatározása.

Általánosan elmondható, hogy a célunk mindig az elégséges, de mégis a lehető legkevesebb jogosultság kiosztása. Ennek az elvnek a betartása a napi gyakorlatban képes igazán kamatozni, hiszen, ha a felhasználók a feladataik elvégzéséhez szükséges összes jogosultsággal rendelkeznek, akkor az informatikai rendszer nem gátolja, hanem elősegíti a magas szintű munkavégzést. Ráadásul ha „csak" a minimálisan elégséges jogosultsággal rendelkeznek, akkor üzemeltetőként vagy a szervezet szempontjából nézve kevésbé kell számolnunk a vétlen vagy szándékos biztonsági problémákkal.



3.2. ábra: *A hitelesítési és engedélyezési folyamat általában egymást követi*

A hitelesítés

A hitelesítés folyamata feltételezi a hitelesítő jelenlétét is, amely a számítógépes környezettől függően többféle lehet, mi most három alappéldát emelnénk ki:

1. **Hitelesítés helyben, azaz interaktív belépéssel az adott számítógépen.** Ekkor a felhasználónak rendelkeznie kell az adott gépen érvényes belépési lehetőséggel, azaz, a gép saját felhasználói adatbázisában valamilyen módon szerepelnie kell a fiókjának. Ekkor tehát az adott gép a hitelesítő, és csak felhasználói fiókokat tud hitelesíteni.
2. **Hálózati hitelesítés**. Elsősorban munkacsoportos környezetben használatos, amikor egy másik a hálózaton jelen levő számítógépre jelentkezünk be (ezt mindig megelőzi a helyi gépre történő belépés). Ennek oka lehet egy megosztott mappa, vagy egy nyomtató elérése. Sok esetben a másik gépre nem ugyanazzal a felhasználónévvel és jelszóval lépünk be, mint helyben, hiszen ilyenkor a másik gép felhasználói adatbázisa a domináns, tehát eltérőek lehetnek a hitelesítő adatok. Ekkor tehát a másik gépet tekinthetjük a hitelesítőnek, amely szintén csak felhasználói fiókokat tud hitelesíteni.

3. **Tartományi hitelesítés**. A legkomplexebb megoldás, amely egyben a legtöbbet is nyújtja. Mivel létezik a tartomány, dolgozik a címtárszolgáltatás, a felhasználók fiókjainak és hitelesítő adatainak tárolása a címtár adatbázisban történik, az engedélyekkel és más információkkal együtt. Alapesetben akármelyik tartományi tagsággal rendelkező számítógépen bejelentkezhetünk a tartományba is (ez is az ajánlott, sőt, sok esetben a helyi belépés ilyenkor nem is lehetséges, nincs is szükség rá), hiszen a tartományvezérlőket ezekről elérjük, amelyek a rajtuk található címtár adatbázis segítségével, központilag képesek hitelesíteni bennünket. De nemcsak az interaktív belépés létezik, tartományban lehetőség van a számítógépfiókok létrehozására és tárolására, a tartománytag gépek rendelkeznek jelszóval is, így ezek is „belépnek", azaz képesek hitelesíteni is magukat. Tartomány esetén tehát a felhasználók és a gépek esetén is a címtárszolgáltatás, illetve ennek konkrét képviselője, a tartományvezérlő a hitelesítő elem.

Akár egy helyi gépről, akár egy hálózatról van szó, a hitelesítés folyamata során a felhasználó jelszavának biztonságos tárolása minden esetben alapvetően szükséges (erre később még visszatérünk). Az utóbbi esetben viszont számolnunk kell még azzal is, hogy adott hálózati forgalomban a legtöbb esetben a hitelesítő adatok szállítás közben védtelenek, azaz megfelelő szoftveres, vagy hardvereszközzel mások számára is hozzáférhetőek, ezért mindenképpen úgy kell „kinézniük", hogy egyáltalán ne jusson előbbre velük az, aki ellopja az adott forgalom részleteit. De e feltételek teljesülése előtt még egy fontos lépcsőfok van: rendelkeznünk kell a hitelesítő adatokkal.

A hitelesítés főszereplői

A rejtélyes cím mögött némiképp puritán tartalom áll, azaz ebben a fejezetben a Windows Vista felhasználói fiókjairól és csoportjairól lesz szó.

Ha nem tartományról beszélünk, hanem önálló vagy munkacsoportos környezetről, akkor a felhasználói fiók *(user account)* az adott gép – kizárólag csak helyben használható – felhasználóját személyesíti meg. A fiók objektum tárolja a felhasználó alapadatait (nevét, csoporttagságát, ikonját stb.), és a legfőbb feladat az, hogy a rendszer erőforrásaihoz hozzáférési jogosultságokat definiáljunk számára, illetve hogy a felhasználók tevékenysége (pl. belépés, fájlhozzáférés stb.) nevesítve jelenjen meg a naplófájlokban. Emellett természetesen az eltérő munkakörnyezet, illetve az egyedi beállítások elérése is célunk lehet, a különböző felhasználói fiókok létrehozása apropóján.

A helyi számítógép viszonylatában a fiókok, a jelszavaikkal, a csoportokkal és az egyéb, pl. biztonsági jellemzőkkel együtt egy speciális, ún. helyi biztonsági adatbázisban tárolódnak *(Security Account Manager)* és amely gyakorlatilag a rendszerleíró adatbázis egyik ágában található meg, de ami egyúttal a *Windows\System32\Config\SAM* fájl tartalma is.

Még mielőtt nekiesnénk a *regedit.exe*-nek, illetve az említett fájlnak, tudnunk kell, hogy kicsit nehezen vizsgálhatjuk meg ezeket még teljes körű rendszergazda jogosultsággal is, hiszen a registry ezen ágához *(HKLM\SAM)* csak a *SYSTEM* felhasználónak van jogosultsága, akinek viszont nincs interaktív belépési lehetősége a gépen. A *SAM* fájl pedig az operációs rendszer működése alatt – számunkra – nem nyitható meg.

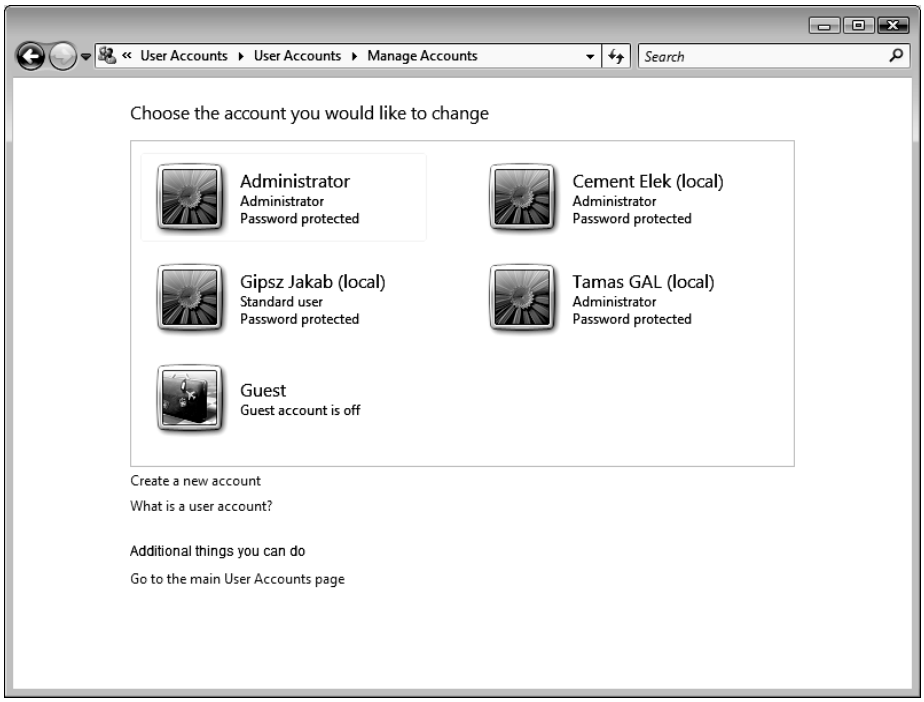
A felhasználói fiókokat mindig felhasználónévvel és, (nem kötelezően, de mégis ajánlottan), jelszóval különböztetjük meg egymástól, de további tulajdonságai is lehetnek – igaz egy helyi fiók esetén viszonylag kevés opcióval rendelkezünk ezen a területen (lásd ugyanebben az alfejezetben, később). Fontos jellemzője viszont az adott fióknak a típusa, amelyből a Windows Vistában két fő, és egy, csak nagyon extrém esetben használtat ismerünk:

1. **Administrator *(Rendszergazda)* fióktípus**: Az Administrators *(Rendszergazdák)* csoport tagjai, magas jogosultsággal használhatják a gépet. Alapértelmezés szerint a telepítés során megadott fiók is ebbe a csoportba kerül, és csak e csoport tagjaként hozhatunk létre, változtathatunk és törölhetünk további felhasználói fiókokat. A teljesség igénye nélkül, nézzük meg, hogy melyek a legfontosabb további műveletek, amelyre csak egy admin fiók birtokában leszünk képesek:
    - bármely felhasználó jelszavának megváltoztatása;
    - alkalmazásokat telepíteni és eltávolítani;
    - a hardver eszközök eszközmeghajtóit telepíteni vagy eltávolítani;
    - mappákat megosztani;
    - engedélyeket és jogosultságokat beállítani más felhasználóknak (vagy önmaguknak);
    - a kötetek összes állományát elérni, más felhasználók fájljait is beleértve;
    - fájlok és mappák tulajdonjogát átvenni;
    - a *Program Files* és a *Windows* mappákba írni;
    - lementett rendszerfájlokat visszaállítani;

- a rendszeridőt és a naptárt beállítani;
- a Windows Tűzfalat konfigurálni;
- beállítani a biztonsági frissítéseket, illetve manuálisan biztonsági frissítéseket telepíteni.

2. **Standard *(Általános jogú)* fióktípus**: A Users *(Felhasználók)* csoport tagjai a korábbi operációs rendszereknél csak egy alapszintű jogosultságcsokorral voltak kénytelenek beérni. A Windows Vista esetében jelentős haladás történt: itt már egy standard felhasználó gyakorlatilag mindenre képes, ami a számítógép napi használatához szükséges – de ha mélyebb, a rendszer biztonságát, működését alapjaiban megváltoztató műveletet szeretnénk elvégezni, akkor rendszergazda segítségére (vagy jogosultságra) lesz szükségünk (részletesebben ezzel a kérdéskörrel a felhasználói fiókok felügyelete *(User Account Control, UAC)* alfejezetben lesz szó). Lássunk néhány konkrét lehetőséget – főképp a viszonyítás kedvéért – amelyekre a Vistán egy standard felhasználó képes:
   - saját jelszó megváltoztatása;
   - a telepített programok használata;
   - hardvereszközök eszközmeghajtóinak telepítése, (ha külön kapunk rá engedélyt);
   - a jogosultságok megtekintése;
   - fájlok létrehozása, változtatása és törlése a saját Dokumentumok mappában, illetve a saját, megosztott mappákban;
   - a személyesen lementett fájlok visszaállítása;
   - a rendszeridő és naptár megtekintése, az időzóna megváltoztatása;
   - az energiaellátási opciók beállítása;
   - belépés csökkentett módban.
3. **Guest *(Vendég)* fióktípus**: A Guests *(Vendégek)* csoportba tartozó fiókok megszemélyesítői nagyon minimális jogosultságokkal rendelkeznek, mélyen a standard felhasználók jogosultsági szintje alatt. Ideiglenes jelleggel és/vagy nagyon korlátozott hozzáférés céljából használjuk. Jó példa erre, hogy az azonos nevű Guest *(Vendég)* fiók tulajdonosa még a saját jelszavát sem hozhatja létre, a Users *(Felhasználók)* csoportnak sem tagja, és alapesetben ez a fiók le is van tiltva.

A felhasználói fiókok kezelése többféle helyen is történhet a Vistában. Az általános opciókat a Control Panel *(Vezérlőpult)* / User Accounts *(Felhasználói fiókok)* alatt találjuk. Önálló vagy munkacsoportos környezetben itt hozhatunk létre új fiókokat, törölhetjük, átnevezhetjük ezeket, megváltoztathatjuk a típusukat és a jelszavakat, vagy akár – megfelelő jogosultsággal – más helyi felhasználók beállításait is korrigálhatjuk. Kapunk lehetőséget a profilunk, a hálózati jelszavaink (lásd egy későbbi alfejezetben) vagy a fájlok titkosításához szükséges tanúsítványok kezelésére is. Ha viszont a gépünk nem önálló, hanem tagja egy tartománynak, akkor itt jóval kevesebb lehetőséget találunk a helyi felhasználói fiókok kezelésére.



3.3. ábra: *Munkacsoportos környezetben így (is) láthatjuk a fiókokat*

A haladó és egyben a klasszikus beállításokat innen – munkacsoportos környezetben – nem érjük el, ellenben a megfelelő MMC-konzol segítségével már igen, méghozzá az első fejezetben már ismertetett Computer Management MMC részeként (Local Users and Groups – *Helyi felhasználók és csoportok).* Ezen a felületen már több lehetőségünk is lesz, például a Users *(Felhasználók)* szakaszon belül, az alapértelmezés szerint egyformán letiltott Administrator *(Rendszergazda)* es Guest *(Vendég)* fiókok mellett meg fogjuk találni a telepítéskor általunk létrehozott fiókunkat is. E fiók tulajdonságlapja körülbelül ugyanúgy néz ki, mint a következő képen.

A Vista különböző változatai alig térnek el a felhasználói fiókok és a csoportok kezelését illetően, különbség maximum az esetleges tartományi tagság miatt a felszínen, azaz a grafikus felületen adódhat. Mivel csak a Business, az Enterprise, illetve az Ultimate változatot léptethetjük be tartományba, ezért a szövegben említett különbség is csak ezeknél a változatoknál fellelhető. Jó tudni viszont, hogy a Vista Home Basic, illetve a Home Premium változata alatt a Local Users and Groups MMC konzol nem elérhető.

3.4. ábra: *Egy felhasználói fiók tulajdonságai*

Itt a név és a leírás mellett a fiók jelszavára vonatkozó beállításokat is láthatunk, ezek a következőek:

- User must change password at next logon *(A következő bejelentkezéskor meg kell változtatni a jelszót)* – A soron következő (vagy akár a legelső) belépéskor a felhasználónak meg kell változtatnia a jelszavát. Ennek értelme akkor van, ha rendszergazdaként nem akarunk jelszót meghatározni a felhasználónak, vagy akkor, ha kifejezetten kényszeríteni szeretnénk arra, hogy megváltoztassa.
- User cannot change password *(A jelszót nem lehet megváltoztatni)* – Ha nem akarjuk, a felhasználó nem változtathatja meg a saját jelszavát. Ritkán, esetleg a közösen használt fiókok esetén van értelme ennek a beállításnak.

- Password neves expires *(A jelszó sohasem jár le)* – A Vista alapbeállítás szerint 42 naponként automatikusan kéri a felhasználótól a jelszó megváltoztatását. Ha itt kikapcsoljuk, akkor mentesülhetünk ettől.

A maradék két lehetőség közül az első a fiók letiltására *(Account disabled)* vonatkozik, ami gyakorlatilag teljesen felfüggeszti, de nem távolítja el a rendszerből az adott fiókot. A második pedig a fiók (többnyire ideiglenes, pl. több helytelen jelszó megadás miatt automatikus) kizárására vagy a már megtörtént kizárás feloldására vonatkozik.

E panel két további füle is fontos tulajdonságokat hordoz:

- A **Member Of** segítségével állíthatjuk be az adott fiók csoporttagságát (ha van hozzá jogosultságunk).
- A **Profile** fülön a felhasználó komplett profiljának lelőhelye szerepel (ha eltér az alapértelmezett, többnyire a *\Users\felhasználó_neve* mappától), illetve a logon szkriptjének (belépési parancsfájl) neve, amely a felhasználó belépésekor lefutó általában kötegelt (pl. *.bat)* állomány megnevezése.
- **Home folder** *(Kezdőmappa):* a felhasználó alapkönyvtárának helye, ez általában a parancssori ablak *(cmd.exe)* kezdőkönyvtára is.

Önálló gép vagy munkacsoport esetén az utóbbi opciókat (a jelszóra vonatkozóakat is beleértve) tipikusan egyáltalán nem használjuk, ezek elsősorban tartományi környezetben alkalmazott beállítások. Igaz, ebben az esetben viszont nem a helyi gépeken, hanem központosítva, a címtárban tárolt felhasználói fiók beállításainak szabályozzuk ezeket a lehetőségeket.

Ennek az alfejezetnek a másik fő témája a már kényszerűségből többször is említett felhasználói csoportok. Az előző rész alapján már tisztában vagyunk azzal, hogy egy helyi gép esetén milyen fő típusok állnak rendelkezésre ezekből (Administrators, Users, Guests), illetve azt is láthattuk, hogy egy-egy felhasználó esetén hol állíthatjuk a csoporttagságot. Tekintsük át most a csoportokkal kapcsolatos további részleteket!

Az összes operációs rendszerben – így a Windows Vistában is – a csoportok létrehozásának célja elsősorban a felhasználók fiókjainak összegyűjtése, közös kezelése. Ha létrehozunk egy csoportot és hozzárendelünk felhasználókat, akkor pl. a jogosultságokat, vagy az engedélyeket egy lépésben, minimális energiával képesek leszünk beállítani az adott felhasználói kör számára. Ezen kívül az objektumokhoz csatolt jogosultsági listák is kisebb méretűek lesznek, tehát gyorsabban dolgozza fel, értékeli ki ezeket az operációs rendszer.

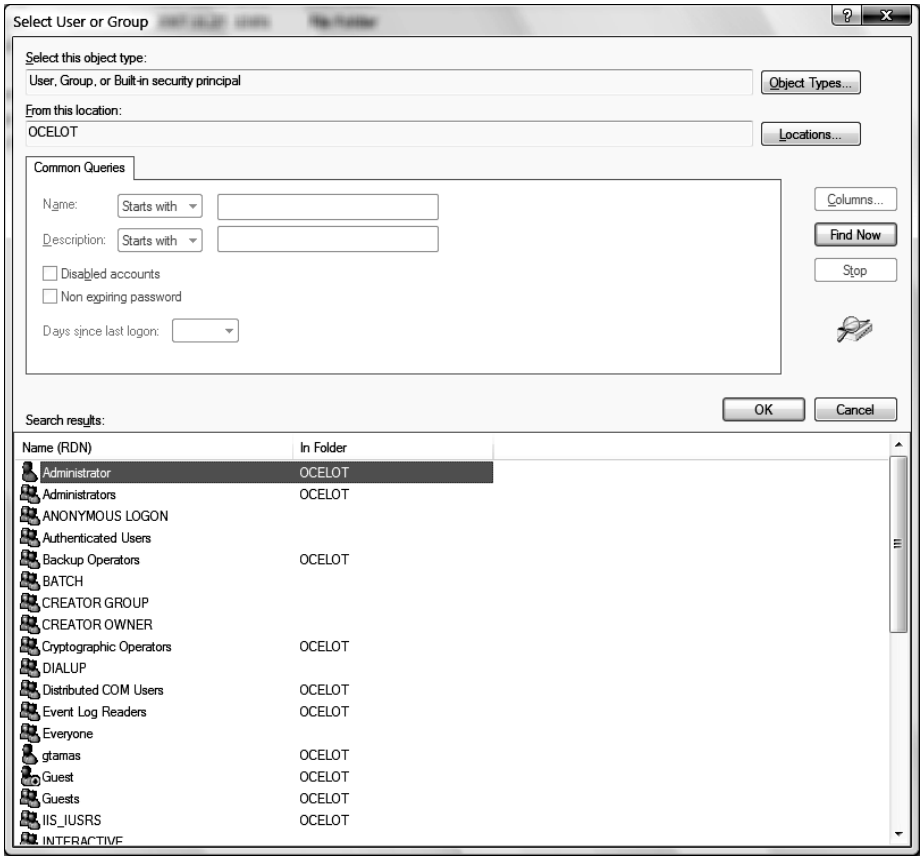
A Windows operációs rendszerek tartalmaznak egy sereg beépített, a telepítés után már elérhető csoportot, ezek fajtáit a következő felsorolásban mutatjuk be (a Vista-specifikus csoportokról, illetve az elsősorban biztonsági okokból történt felhasználói és csoportváltozásokról egy későbbi alfejezetben nyújtunk majd egy részletes áttekintést).

- **Administrators** *(Rendszergazdák):* A rendszergazdák csoportja, elvileg majdnem az összes művelet és feladatkör birtokosa az operációs rendszerben.
- **Backup Operators** *(Biztonságimásolat-felelősök):* E csoport tagjai biztonsági mentéseket és visszaállításokat végezhetnek el, azaz ebből a célból a kötetetek összes objektumához hozzáférnek.
- **Guests** *(Vendégek):* minimális jogkörrel rendelkező, speciális csoport, egyetlen tagja alapértelmezés szerint a már említett Guest fiók.
- **Network Configuration Operators** *(Hálózat-beállítási felelősök):* A hálózati szolgáltatások közül bizonyos – egyébként rendszergazdai – műveletek (TCP/IP -konfigurálás, hálózati kapcsolatok engedélyezése, DNS-cache ürítése, RAS-kapcsolatok legyártása, törlése stb.) ellátására is képesek lesznek e csoport tagjai.
- **Remote Desktop Users** *(Asztal távoli felhasználói):* Az első fejezetben említett Remote Desktop *(Távoli asztal)* szolgáltatás felhasználói, akik jogosultak elérni az adott gépet a Remote Desktop ügyfélprogrammal.
- **Replicator** *(Replikáló):* Fájlok, mappák tartományon belüli replikációját teszi lehetővé a csoport tagjai számára.
- **Users** *(Felhasználók):* A már többször említett csoport tagjai az átlagos, standard típusú felhasználói fiókok. Minden új fiók alapértelmezett tartózkodási helye is ez a csoport.

Ha alaposan megvizsgáljuk az operációs rendszert példaképpen az adható jogosultságok és engedélyek kapcsán, akkor további, sok esetben nagyon ritkán használt, speciális csoportokra is rábukkanhatunk.

Ezek a csoportok nem láthatóak a Local Users and Groups *(Helyi felhasználók és csoportok)* MMC-ben, és a tagsági viszonyaikat sem állíthatjuk be a felhasználói felületről (az operációs rendszer végzi ezt el helyettünk), viszont szükség esetén adhatunk ki számukra fájlokra és mappákra jogosultságokat, illetve kaphatnak egyéb engedélyeket is. Ezeket a jogosultság- vagy engedélyhozzárendeléseket viszont általában nem nekünk kell manuálisan megtennünk, a gyári alapbeállítások tartalmazzák e csoportok hozzárendelését a szükséges erőforrásokhoz, objektumokhoz, illetve folyamatokhoz. Tekintsük meg e csoportok listáját is, egy-egy rövid jellemzéssel kísérve a felsorolást:

- **Everyone** *(Mindenki):* Ennek a csoportnak az összes felhasználói fiók és egyéb, speciális felhasználó tagja (az Anonymous Logon csoport tagjai kivételével). Tisztában kell lennünk azzal a ténnyel, hogy ha ennek a csoportnak adunk pl. egy mappán jogosultságot, akkor az az összes helyi, vagy távoli hozzáférés esetén érvényes lesz. Épp ezért e csoport használata (még ha igen kényelmes is), nem ajánlott. Még akkor sem, ha a Windows XP-ben e csoport számára általánosan megkapott Read *(Olvasás)* jogosultság a Vistában már nem biztosított.



3.5. ábra: *A speciális, csak a jogosultság kiosztáskor használatos csoportok*

- **Authenticated Users** *(Hitelesített felhasználók):* az Everyone, illetve a Users csoportokhoz képest egy zártabb csoport, amely egyrészt az Everyone-nal szemben nem tartalmazza a Guest *(Vendég)* felhasználót, az Usersszel szemben pedig csak a valóban hitelesített felhasználókat tartalmazza. Minden felhasználó tagja lehet, aki helyben jelentkezett be, a hálózatból vagy telefonos kapcsolaton keresztül használja a szá-

mítógépet. Íratlan szabály, hogy manuális jogosultságkiosztásnál, ha minden interaktív felhasználónak akarunk jogot adni, egy erőforráshoz, akkor azt mindig ezen a csoporton keresztül tesszük meg.

- **Anonymous Logon** *(Névtelen bejelentkezés):* E csoport tagjai szerény lehetőségekkel vannak felvértezve, mivel olyan „felhasználókról" van szó, akik nem azonosították magukat névvel és jelszóval. Ilyen „felhasználó" viszonylag kevés van, ide tartozik pl. az ún. *null session*ön keresztüli elérés (pl. a gépek kommunikációja esetén az IPC$ megosztás használata, lásd később). Helyi alkalmazása alapértelmezés szerint viszont tiltott.
- **Batch** *(Köteg):* Azon felhasználók, akik a nélkül indíthatnak el parancsfájlokat, hogy interaktívan bejelentkeznének (pl. egy program futtatásának időzítése).
- **Creator Owner** *(Létrehozó tulajdonos),* Creator Group *(Létrehozó csoport):* Az erőforrások alapértelmezett jogosultsági listájában rendszeresen találkozhatunk e fiókkal, illetve csoporttal, amelyek az adott objektum tulajdonosát jelölik, azaz azt a felhasználót, aki létrehozta az erőforrást. A Creator Group használata a Windows operációs rendszerekben nem jellemző, elsősorban a POSIX kompatibilitás miatt szükségesek.
- **Dialup** *(Telefonos):* Azokat a felhasználókat jelöli meg az operációs rendszer ebbe a csoportba tartozó tagnak, akik aktuálisan a telefonos hálózaton keresztül csatlakoznak a számítógéphez.
- **Interactive** *(Interaktív):* Azon felhasználók a tagjai ennek a csoportnak, akik képesek manuálisan (a felhasználónév/jelszó párossal) belépni az operációs rendszerbe, beleértve a Remote Desktop *(Távoli asztal)* szolgáltatást használókat is.
- **Network** *(Hálózat):* A hálózaton keresztül kapcsolódó felhasználók, akik tipikusan a helyi gép egy megosztott erőforrásához kapcsolódnak.

A felhasználók és a csoportok kezelése a parancssorból is megoldható. A *net user* és a *net localgroup* parancsoknak számtalan, jól használható paramétere van.

A hitelesítés protokolljai

A hitelesítést többféle protokoll segítségével bonyolíthatjuk le, ezek különbsége elsősorban a hitelesítés során használt jelszavak tárolási módszerében, kisebb számú esetben a továbbításuk módszerében jelentkezik. Az eléggé elterjedt hiedelemmel ellentétben a Windows operációs rendszerek nem tárolják el a jelszavakat, pontosabban nem a jelszavakat tárolják el, hanem az ezekből

speciális tördelőalgoritmusokkal képzett kivonatokat, más néven hash-eket. Egy ilyen kivonat mindig teljesen egyedi, így használható a jelszó helyett, viszont magából a kivonatból semmilyen körülmények között nem lehetséges visszaállítani az adott jelszót.

Egy adott hash birtokában egyetlen módszerünk a jelszó kitalálására a próbálgatás és összehasonlítás, azaz sok-sok jelszó kivonatának elkészítése, majd az ezek összehasonlítása a feltörendő jelszó kivonatával. Ezt a szaknyelvben „brute force" módszernek hívjuk.

A jelszavak tárolási módszere tehát kulcsfontosságú a hitelesítés szempontjából. A régebbi hitelesítési megoldások mellőzésének oka pontosan az, ami általában a legfőbb kritérium is ezekkel a módszerekkel szemben: mennyi ideig képesek ellenállni a feltörés kísérletének. Mivel a feltöréshez szükséges szoftverek kódjában matematikai műveletek dominálnak, ahogy nő az ezekhez szükséges hardverelemek (CPU, RAM stb.) teljesítménye, úgy csökkenhet a törésre fordított idő. Mikor tekinthetünk egy módszert tényleg biztonságosnak? Erre kivételesen van általános érvényű szabály: ha a védett adatok megszerzéséhez szükséges idő (nagyságrendekkel) több, mint amennyi ideig biztonságban szeretnénk tudni az adott adatokat.

A következő lista elemei közül néhány már nincs, vagy alig van használatban, de esetleg a kompatibilitás miatt szükségesek lehetnek.

- **LAN Manager (LANMAN)** – Eléggé egyszerű jelszótárolással (LM hash) operáló hitelesítési módszer, a régebbi Windows 3.1x/95/98/Me, illetve MS-DOS operációs rendszerekben volt használatos. A jelszavak kivonatának elkészítése során olyan kényszerű hiányosságokkal rendelkezik, amelyek miatt ma már egyszerűen és gyorsan lehetséges a megfelelő teljesítményű hardverrel feltörni. A példa kedvéért nézzük meg, hogyan készül el egy LM hash:

    1. A jelszó nagybetűsítése (tehát teljesen mindegy, hogy felváltva használunk-e kis- és nagybetűket!)
    2. A jelszó kiegészítése szóközökkel, 14 bájt hosszúságra (tehát, ha egy 9-karakteres jelszavunk van, akkor gyakorlatilag egy 7 és egy 2 karakterből álló részt kell feltörni, mivel az utolsó 5 karakter tuti, hogy szóköz lesz!)
    3. A 14-bájtos jelszóból ($14 \times 8 = 112 = 2 \times 56$ bit) 2 db DES kulcs készül.

4. A két 56-bites DES kulccsal titkosítunk egy mindig állandó (!) sztringet *(KGS!@#$%)*.
5. Az eredmény 2 × 8 bájt, összesen tehát egy 16-bájtos hash.

Látható, hogy több furcsa anomália is jellemző erre tárolási módszerre, amelyek nagyban segítenek a brute force alkalmazásoknak, hogy pillanatok alatt elérjék a céljukat, ezért aztán a LANMAN hitelesítés ma már tényleg teljesen elavultnak számít és veszélyes a használata.

- **NTLMv1** (NT LAN Manager v1) – Kérdés-válasz *(Challenge/Response)* elven működő autentikációs protokoll. Az NTLM használatakor a hitelesítést kérő ügyfél egy véletlenszerűen generált 8-bájtos „kihívást" *(challenge)* kap a kiszolgálótól, melyet aztán a felhasználó jelszavával titkosít és visszaküld, némiképp feltupírozva, összesen 2 × 24 bájtban. Az NTLMv1 protokollt tipikusan a Windows NT 4 SP4 előtti rendszerekben alkalmazták, és ma már szintén nem nyújt elégséges védelmet, hiszen amellett, hogy egyrészt az MD4 (Message Digest 4) algoritmust használja az NT hash elkészítéséhez (ami anno elég erős titkosításnak számított), az iménti ismerős, az LM hash is ugyanúgy része lesz a válasznak, és így nem jutunk sokra vele.
- **NTLMv2** – Az első verzió kriptográfiailag megerősített változata, a Windows NT 4 SP4 javítócsomag óta használhatjuk, a későbbi rendszerek természetesen már alapértelmezésben tartalmazzák. Ha nem áll rendelkezésre a Kerberos protokoll (pl. webes hitelesítésnél vagy tartományon kívül, vagy ha IP-cím alapján kell hitelesíteni), akkor tökéletesen megfelelőnek tekinthető, hiszen „erősségét" tekintve gyakorlatilag az NTLMv2 számít az összes módszer közül a legjobbnak: 128-bites kulcsteret használ, külön-külön kulcsokkal az üzenet hitelesség és integritás biztosítására, és az MD4 helyett a HMAC-MD5 kivonatokkal operál.

Egyes hash-algoritmusok lehetővé teszik, hogy paraméterezzük őket, azaz a kimenetüket kicsit megváltoztathatjuk, amelyet sózásnak *(salted)* is hívnak. Ez a módszer lehetővé teszi, hogy a hash mindig egy kicsit másmilyen legyen, ezzel is nehezítve az ellopás lehetőségét. A korábban említett 8-bájtos kihívás pontosan erről szól, de ez csak a kezdet. Ma az egyik legjobb „sószóró" a HMAC algoritmus (Hash Message Authentication Code), melyet úgy terveztek, hogy a meglévő és bevált algoritmusokkal változtatás nélkül együttműködjön. Így jöhet létre a HMAC-MD5, amely nevéből kitalálható, hogy a HMAC egy komoly preparálást végez az adatokon, s ennek az eredményét juttatja el az eredeti MD5 algoritmushoz.

Mindkét NTLM-hitelesítési protokoll közös hátránya viszont a relatíve nagyobb hálózati forgalom generálása, amely például a kivonatok minden egyes alkalommal történő elküldésében nyilvánul meg, és ez egyben emiatt nagyobb sebezhetőséget is jelent.

- **Kerberos V5** – A Microsoft a Kerberost (pontosabban ennek V5-ös verzióját) választotta a címtárszolgáltatás alapértelmezett hitelesítési protokolljává a Windows 2000 Serverben, és ez azóta sem változott. A Kerberos főbb előnyei közé tartozik a platformfüggetlenség (mivel egy RFC-ben rögzített típusú hitelesítési módszerrel állunk szemben), a minimális hálózati plusz forgalom, valamint a biztonsági házirendből történő konfigurálhatóság.

- A Kerberos V5 nélkülözhetetlen szolgáltatása a kulcsszolgáltató központ *(Key Distribution Center – KDC),* mely Active Directory címtárszolgáltatás részeként minden tartományvezérlőn fut. A KDC felel a jegyek küldésekor használt titkosítókulcsok generálásáért és folyamatos üzemeltetéséért. A KDC az összes további a tartományvezérlőkön futó biztonsági szolgáltatással integrálva van, illetve az AD adatbázisát, (illetve a globális kalatógust is) használja saját adatbázisaként.

  A Kerberos V5 hitelesítési folyamata egyszerűsítve a következőképpen működik (természetesen az egész hitelesítési folyamat láthatatlan a felhasználó számára):

  1. Az ügyfélgépen belépni szándékozó felhasználó – jelszó és/vagy intelligens kártya használatával – hitelesíti magát a szintén a tartományvezérlőkön futó összetevő, a hitelesítésszolgáltató *(Authentication Service – AS)* felé.

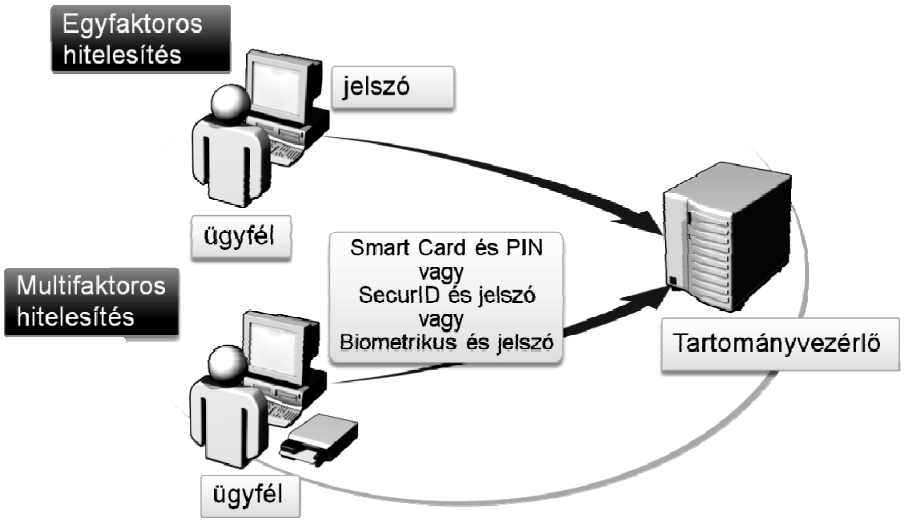
  2. Az AS leellenőrzi a felhasználót az AD segítségével, majd felveszi a kapcsolatot a KDC-vel az új kulcs legyártása érdekében.

  3. A KDC egy egyedi *(session)* kulcsot biztosít az ügyfélnek. Az AS ezt egy speciális jeggyel *(Ticket Granting Ticket – TGT)* együtt küldi el a felhasználónak. A TGT azért is fontos (az ügyfél el is tárolja), mert a további jegyeket is ezzel lehet majd kérni, immár anélkül, hogy a jelszóra/felhasználónévre szükség lenne. Ez a kedvezmény persze nem tart örökké, alapbeállítás szerint mindösszesen csak 10 óráig.

  4. Az ügyfél a nála lévő TGT felhasználásával jegyet kér és kap a harmadik fontos kiszolgálóoldali komponenstől, a Ticket Granting Service-től (TGS).

5. Végül az ügyfél ezt a jegyet mutatja be a kért hálózati szolgáltatásnak (azaz az NTLM-mel ellentétben nem utazik minden alkalommal a jelszó kivonat a hálózaton!), pl. jelen esetben a tartományi belépést kontrolláló tartományvezérlőnek, és kap engedélyt a tartományi belépésre. Ha ezek után az adott 10 órán belül valamilyen más szolgáltatás esetén újra igazolnia kell magát, akkor a letárolt TGT-vel megint kér egy szolgáltatásjegyet, és aztán csendben ezt bemutatja a kérő felé.

A Kerberos V5-szolgáltatás minden tartományvezérlőn, a Kerberos-ügyfél pedig minden munkaállomáson alapértelmezésként telepítve van, és aktív. Minden tartományvezérlő kulcsszolgáltatóként működik, az ügyfelek hitelesítéskor DNS-lekérdezéssel keresik meg a legközelebbi tartományvezérlőt. A bejelentkezés során ez a megtalált tartományvezérlő szolgál kulcsszolgáltatóként a felhasználó számára. Ha az elsődleges kulcsszolgáltató elérhetetlenné válik, a rendszer új kulcsszolgáltatót keres a hitelesítés végrehajtásához. Ha egyetlen kulcsszolgáltató sem elérhető, a belépés meghiúsul.



3.6. ábra: *A multifaktoros hitelesítés előnyei könnyen beláthatók*

A felhasználók hitelesítése egy- vagy többfaktoros módszerrel is történhet. Többfaktoros hitelesítésnek nevezzük azt az azonosítási metódust, ahol nem csak egy név/jelszó párossal, hanem egyéb rendelkezésre álló eszközökkel, például intelligens kártyával, vagy egyéb hitelesítő hardverkulccsal (pl. SecurID-eszközök), egyaránt azonosítjuk magunkat.

A multifaktoros hitelesítés lényegesen biztonságosabb belépést tesz lehetővé, hiszen a felhasználót nemcsak jelszava, vagy kódja azonosítja – mely esetleg kitalálható, vagy más egyszerű módon megszerezhető – hanem a fizikailag birtokolt eszköz is. Ilyenkor tehát nemcsak „tudunk valamit" (a jelszót), hanem a „van valamink" elv is érvényesül.

Az intelligens kártya (SmartCard) használata esetén a felhasználónak a kártya PIN-kódját kell csak ismernie, és a bejelentkezéskor szükséges a kártya is. A PIN-kód lehet egyszerű is (pl. 4 karakter), de ez nem gond, mivel nem megy át a hálózaton, hanem a Crypto API-n egyenesen áthaladva a kártyához tartozó Crypto Service Provider segítségével lejut az eszközbe. Ez az útvonal eléggé biztonságos, gyakorlatilag lehallgathatatlannak tekinthető.

Ráadásul a kártyák általában rendelkeznek „önmegsemmisítő" szolgáltatással, vagyis X darab sikertelen bejelentkezés után használhatatlanná válnak, illetve le is járhatnak, azaz Y idejű inaktivitás után szintén nem használhatóak.

A Windows világban a kiszolgáló és ügyfél oldali operációs rendszerek és alkalmazások (Active Directory címtár, ISA Server, Vista stb.) többféleképpen támogatják a multifaktoros hitelesítési típusokat is, van, amelyiket teljesen integráltan (pl. az intelligens kártyák), és van, amelyeket csak közvetítő, továbbító közegként, egy-egy külső, külön telepíthető alkalmazás felé (pl. RSA SecurID).

A jogosultságok

A jogosultságok definiálják a hozzáférés típusát egy erőforráshoz, vagy másképp fogalmazva, a sikeres hitelesítés után a jogosultságok alapján határozhatjuk meg, hogy például a felhasználó vagy a számítógép az adott objektumokkal milyen műveleteket végezhet. Tehát az engedélyezés (autorizáció) folyamatának az alapját jelentik. A jogosultságokat mindig az objektumokon érvényesítjük, melyek listáját az alábbi felsorolásban foglaltuk össze (a következő alfejezetekben pedig részletezzük is ezeket):

- NTFS-lemezeken tárolt fájlok és mappák;
- mappamegosztások a hálózat felhasználói számára (a helyi felhasználóknak is lehetséges, csak kevés értelme van);
- megosztott nyomtatók helyi és hálózati felhasználók számára.

Jogosultságokat a lista elemein kívül beállíthatunk más rendszerobjektumok esetén is, pl. a rendszerfolyamatok (processzek), rendszerszolgáltatások (szervizek), a registrykulcsok és -bejegyzések, vagy akár tartomány esetén a címtárszolgáltatás objektumain is.

Az azonosítás (pl. a rendszerbe való belépés) után a felhasználó egy testre szabott ún. *access token*t kap, ami tartalmazza jogosultságait, csoporttagságát stb. A különböző szolgáltatást nyújtó eszközök később ezt az access tokent ellenőrzik, majd ennek tartalma alapján döntik el, hogy a felhasználó hozzáférhet-e egy erőforráshoz (megosztott fájlhoz, számítógéphez stb.), vagy sem. Az egy-egy objektumhoz rendelt hozzáféréseket úgynevezett hozzáférési listákban *(Access Control List – ACL)* rögzítik. Az operációs rendszer az ACL-ek alapján engedélyezi vagy tagadja meg a hozzáférést az objektumokhoz, az ACL-ek pedig úgynevezett Security Identifierek (SID) segítségével azonosítják a felhasználót vagy a számítógépet. Az egyedi SID-eket a hitelesítő információkat tároló kiszolgáló generálja, azaz például a helyi gép, vagy éppen a tartományvezérlő.

A Security Identifierek felépítése a következőképp alakul: (például: *S-1-5-12-7623811015-3361044348-030300820-1013*, részeit egy táblázatban foglaljuk össze).

S	A karakterlánc biztonsági azonosító voltát jelöli
1	Felülvizsgálati szint, az értéke állandó
5	Az azonosító hozzáférési értéke
12-7623811015-3361044348-030300820	A tartományi vagy helyi számítógép-azonosító
1013	A relatív ID (RID), minden nem beépített (tehát létrehozott) felhasználó vagy csoport RID-je 1000-nél nagyobb lesz.

Ahogyan már említettük, a Windowsban több előre definiált felhasználói-, szolgáltatásfiók, illetve felhasználói csoport is létezik, ezek SID-jei minden esetben állandóak, így a gyakorlottabb rendszergazdák akár a név láthatósága nélkül is azonosíthatják ezeket (például eseménynaplókban, hibakereső szoftverekben). A legfontosabb „közismert" (más néven: *well-known)* SID-ek a következők:

S-1-5-18	LocalSystem szolgáltatásfiók
S-1-5-19	LocalService szolgáltatásfiók
S-1-5-20	NetworkService szolgáltatásfiók

S-1-5-21- <tartomány hash-e> -500	Administrator (Rendszergazda) felhasználó
S-1-5-21- <tartomány hash-e> -501	Guest (Vendég) felhasználó
S-1-5-21- <tartomány hash-e> -512	Domain Admins (Tartománygazdák) csoport
S-1-5-21- <tartomány hash-e> -514	Domain Guests (Tartományi vendégek) csoport

A beépített *(built-in)* felhasználók és csoportok SID-jének teljes listáját a Microsoft KB243330 számú tudásbáziscikke sorolja fel. (http://support.microsoft.com/kb/243330)

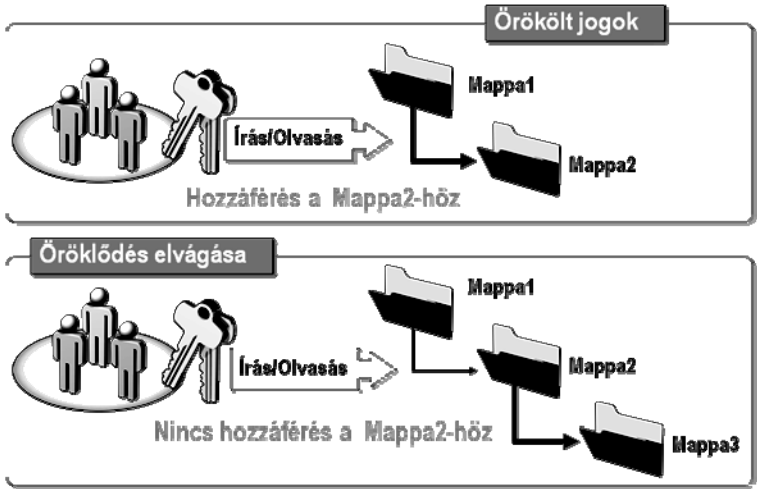
A SID-ek lekérdezésére használhatjuk az integrált *whoami* parancsot, többféle paraméterrel is, pl. a *whoami/user* az aktuális felhasználó SID-jét mutatja meg. Az objektumok ACL-jeit és minden egyéb jogosultsággal kapcsolatos információját az ún. Security Descriptor tárolja. Egy objektum Security Descriptorja a következő elemeket foglalja magába:

- tulajdonos SID-je;
- csoport SID-je (az objektum elsődleges csoporttagságát adja meg, a Windows általában nem használja);
- hozzáférési listák:
    - DACL (Discretionary Access Control List): a felhasználók és csoportok konkrét jogosultsági szintjeit határozza meg, azaz, hogy ki, mit tehet meg pl. az adott fájllal.
    - SACL (System Access Control List): a hozzáférések naplózási módját határozza meg, azaz, hogy kinek milyen sikeres vagy éppen sikertelen, az objektumon végzett műveletét kell naplózni.
- bejegyzések *(Access Control Entry, ACE):* egy-egy konkrét jogosultsági bejegyzés az adott hozzáférési listában (például: *Everyone – Read).*

A fájlrendszer-jogosultságok

A Windows operációs rendszerek tipikus fájlrendszere, az NTFS esetén a jogosultságokat több különböző szempont szerint csoportosíthatjuk, ezek egyike a művelet típusa, melyekre a következő példák hozhatóak fel:

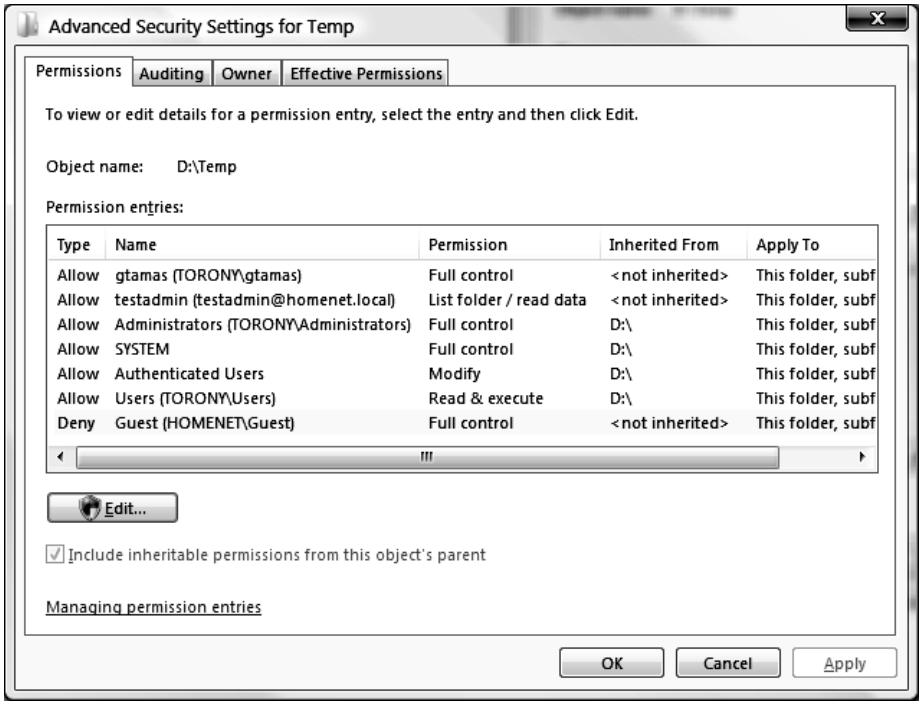
- **Engedélyezett**: az adott felhasználó/gép számára az objektumhoz az adott művelet engedélyezett.
- **Megtagadott**: A tiltás mindig magasabb rendű, mint az engedélyezés, ezért, ha mindkét opció be van jelölve, a tiltás érvényesül.
- **Nincs megadva**: a jogosultság alapértelmezésként nincs definiálva, hatása egyenértékű a tiltással.
- **Öröklött:** az objektum a szülőobjektum (egy vagy több szinttel feljebb lévő gyűjtőobjektum) jogosultságaival rendelkezik. Az öröklött jogosultsági beállításokat általában kiszürkített vagy teli jelölődobozok mutatják. Az öröklődési ágat megszakíthatjuk, azaz egy alsóbb objektumnál egyéni hozzáférést konfigurálhatunk, ekkor az alsóbb objektumnál exkluzív módon adhatunk hozzá, vagy vehetünk el jogosultságot.



3.7. ábra: *Az alapértelmezett jogosultság öröklődés megszüntethető*

A fájlrendszer-jogosultságokat elsősorban a grafikus felhasználói felületről kezeljük – amennyiben megvan a kellő hozzáférésünk az objektumhoz. A változtatáshoz egyszerűen kattintsunk jobb gombbal az elemre, majd válasszuk a Properties *(Tulajdonságok)* parancsot és váltsunk a Security *(Biztonság)* fülre. Itt az egyes hozzárendelt felhasználókat és azok alapvető érvényes jo-

gosultságait tekinthetjük és változtathatjuk meg, de áttekinthetőbb és kezelhetőbb listát kapunk az összes biztonsági beállítással együtt, ha az Advanced *(Speciális)* gombra kattintunk. Nézzünk egy konkrét példát, azaz egy mappa jogosultsági listáját



3.8. ábra: *Példa a jogosultsági listákra*

1. A *TORONY\gtamas* felhasználónak teljes jogosultsága *(Full control)* van a mappán, és nem örökölte *(not inherited)* hanem manuálisan kapta. Ez a mappa egy tartományba léptetett gépen található, ennek ellenére a helyi gép *(TORONY)* egy csoportjának vagy felhasználójának is adhatunk jogosultságot

2. A *testadmin* felhasználó tartományi felhasználó, de ettől függetlenül ő is kaphat jogokat a helyi gépen, de neki csak olvasási joga van, írás nincs, valamint az is látható, hogy az ő jogosultsága sem öröklődő.

3. *TORONY\Administrators* csoportnak szintén teljes jogosultsága van az adott mappán. Az érdekes ebben az, hogy ebbe a csoportba beletartozik a *testadmin* felhasználó is, ergo az előző sor teljesen felesleges. Emellett az is látszik, hogy ez a csoport a *D:* meghajtó gyökerétől kapja öröklés útján ezt a jogosultságot, automatikusan.

4. A *SYSTEM* nevű fiók magát az operációs rendszert, pontosabban a rendszerszolgáltatásokat testesíti meg, ennek megfelelően minden jogosultsága megvan, ami csak létezik *(Full Control)*.
5. Az Authenticated Users *(Hitelesített felhasználók)*: Ez a csoport az adott mappán módosítási joggal rendelkezik, tehát egy fokkal magasabbal, mint a szimpla Users csoport.
6. A *TORONY\Users* csoport tagjainak olvasási joga van. Nem látszik a képen, de ebbe a csoportba beletartozik a *gtamas* es a *gjakab* nevű felhasználó is. Mégis különbözőek lesznek a jogaik, mert a második sorban külön, engedékenyebb szabályzást kapott a *gtamas*, míg a *gjakab* nem, tehát rá a csoportnak adott egyszerű olvasási jog vonatkozik csak.
7. A *HOMENET\Guest* csoport tagjainak nem öröklődő, viszont mindent tiltó jogosultsága van. Ez akkor is így lenne, ha egy másik sorban kapott volna bármilyen engedélyt is ez a csoport, hiszen a tiltás „mindent visz".

Egy fontos dolgot – amelyről már volt szó korábban – immár konkrétan is megfigyelhetünk: a jogosultságokat általában a csoportoknak osztjuk, jelen példában csak a jobb magyarázhatóság kedvéért vettem fel a listába a *testadmin* és a *gtamas* felhasználókat, egyébként alapértelmezés szerint is csak csupa csoportot láthatnánk. Ennek az elvnek alapos oka van, ti. lényegesen könnyebb utólag bevenni egy felhasználót egy csoportba, mint 10, 20 stb. helyen egyesével berakni a szükséges jogosultsági listákba.

Egy másik megfontolandó, és szintén íratlan szabály az, hogy az átláthatóság és az egyszerűbb kezelés miatt nem fájloknak, hanem a fájlokat tároló mappáknak osztunk engedélyeket. Az öröklődést viszont a legritkább esetben kapcsoljuk ki, inkább tervezzük meg alaposan a hatását. Szintén csak indokolt esetben használatos az explicit tiltó (Deny) jogosultság, általában bőven elegendő, ha az adott csoport/felhasználó implicit tiltást kap, azaz nem szerepel a jogosultsági listában.

Ha viszont nem ragadunk le a Permissions *(Engedélyek)* első jogosultsági ablakánál, akkor több érdekes és fontos lehetőségre is rábukkanhatunk ezen az ablakon belül, nézzük meg ezek részleteit is:

- **Permissions fül / Edit...** *(Szerkesztés)* – A jogosultságok részletes beállítására, valamint például az öröklődés megváltoztatására is lehetőségünk nyílik. Két opciónk van itt:
    - **Include inheritable permissions from this object's parent** *(Szülőobjektum örökölhető engedélyeinek hozzávétele)* – A jelenlegi, örökölt jogosultságok teljesen eltávolíthatóak, vagy lemásolhatóak és szerkeszthetőek szabadon.

- **Replace all existing inheritable permission on all descendants with inheritable permissions from this object** *(A meglévő örökölhető engedélyek lecserélése az ezen objektumtól örökölhető engedélyekre az összes gyerekobjektumon)* – azaz az adott szinten lévő jogosultságok „lefelé" (almappákba és fájlokra) történő erőszakos kikényszerítése.

- Ha erről a pontról visszalépünk egyet, akkor elnavigálhatunk az Auditing *(Naplózás)* fülre is, ahol az adott mappa vagy fájl hozzáférésének naplózását állíthatjuk be. Néhány tudnivaló ehhez a lehetőséghez:
  - Alapértelmezésben csak a rendszergazda-csoport tagjaként tehetjük meg az auditálás beállítását.
  - A lista kialakítása ugyanúgy működik, mint a jogosultságoknál.
  - Az öröklődés elvágása és kikényszerítése is ugyanazt a módszert követi.
  - Az eredményt az eseménynaplóban találjuk, konkrétan a Security *(Biztonság)* naplóban.
  - A fájlrendszer hozzáféréseinek naplózásához nem elég itt beállítani a paramétereket, globálisan is engedélyezni kell ezt a lehetőséget. Ezt a helyi vagy a csoportházirendben tehetjük meg, a Audit Policy *(Naplórend)* opciók között az Audit object access *(Objektum-hozzáférés naplózása)* beállításával.
- Lépjünk tovább, és tekintsük meg az Owner *(Tulajdonos)* fül tartalmát.
  - Itt megvizsgálhatjuk, illetve megfelelő jogosultsággal módosíthatjuk az adott objektum tulajdonosi viszonyait, lévén minden egyes erőforrásnak (a hálózati megosztások kivételével) létezik tulajdonosa is. Ha például a felhasználó létrehoz egy mappát, akkor automatikusan ő válik a tulajdonossá.
  - Érdekes jellemző, hogy annak ellenére, hogy a tulajdonosi viszonnyal nem feltétlenül jár együtt a legmagasabb jogosultság, (ha van egyáltalán bármilyen is), viszont a jogokat gond nélkül kioszthatja másoknak.

Rendszerfelügyeleti szempontból lényeges dolog, hogy a tulajdonos „ész nélküli" jogosultságosztogatási lehetőségét fékezve, a rendszergazdacsoport tagjai rendelkeznek a Take Ownership *(Saját tulajdonba vétel)* jogosultsággal. Ez akkor is így van, ha a tulajdonos letilt bennünket. Ez azért fontos, mert néha – mikor mint üzemeltetők nem szerepelünk a jogosultsági listában és nem vagyunk tulajdonosok sem – ezzel a joggal felvértezve, a saját tulajdonbavétel lesz a mentsvárunk a fájl biztonsági beállításainak megváltoztatására.

- A következő fül, az Effective Permission *(Hatályos engedélyek)* egy kifejezetten hasznos eszköz, amellyel egy a rendszerben lévő tetszőleges felhasználó vagy csoport konkrét és aktuális jogosultságait kilistázhatjuk, az adott mappára vonatkozóan. Ezzel pillanatok alatt kiderülhet, hogy az esetlegesen jól összekuszált csoport-, illetve egyénileg kapott jogosultságok halmazának mi a végeredménye.

A fájlrendszer hozzáférés szabályzása

Minden objektum egyedi, rá jellemző hozzáférési listával rendelkezik, amelyek beállítási részleteit és lehetőségeit már bemutattuk. A konkrét jogosultságok ismertetése viszont még hátravan. Ebben az alfejezetben a mappák, és a fájlok jogosultságairól lesz szó, de a hálózati és a nyomtatási jogosultságokra is kitérünk a következő részekben.

A fájlrendszerhez, (csak az NTFS-ről beszélünk), kapcsolódó jogosultságoknál viszont szét kell választanunk a fájlokra és a mappákra vonatkozó lehetőségeket. Ezen a területen a mappákra vonatkozó opciók szélesebb körűek, ennek oka elsősorban az, hogy azok további mappákat, illetve fájlokat is tartalmazhatnak, azaz összetettebb felépítésűek. Ha jó alaposan megnézzük a 3.8. ábrát (117. oldal), akkor azt vehetjük észre, hogy az összes kiosztott jogosultság az adott mappára, az almappáira és a bennük lévő fájlokra érvényes – ez részben kiderül az *Apply to* oszlopból. De nem feltétlenül kell, hogy ez így legyen, tetszés szerint szűrhetjük a jogosultságokat e szerint a hármas tagozódás szerint, bármelyik szinten a mappák között.

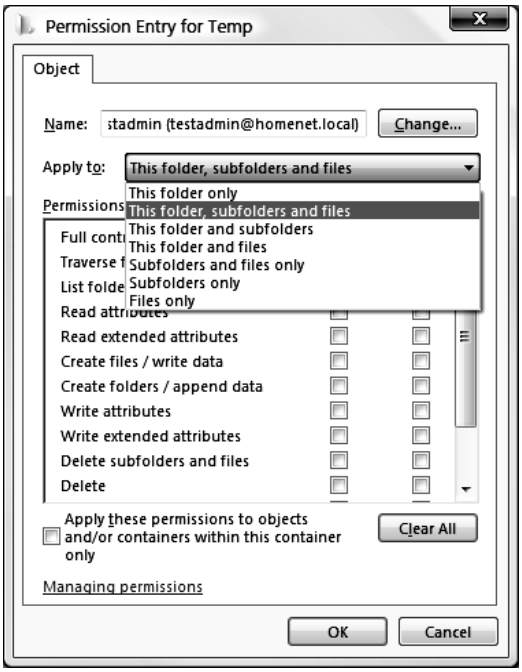
A mappákon állítható alap jogosultságok a következőek:

- **Write** *(Írás):* Fájlok, almappák létrehozása, módosítása, attribútumaik megváltoztatása, írás meglévő fájlokba.
- **Read** *(Olvasás):* A mappa tartalmának listázása, fájlok, mappák és attribútumok olvasása.
- **List Folder Contents** *(Mappa tartalmának listázása):* A Read jog, plusz a könyvtár „bejárása”, valamint az ACL-listák elolvasása.
- **Read and Execute** *(Olvasás és végrehajtás):* Az előző két jog együttese, plusz a fájlok futtatása

- **Modify** *(Módosítás):* A Write + a Read and Execute együttese
- **Full Control** *(Teljes hozzáférés):* Minden létező jogosultság

Azt is tisztán kell látnunk, hogy ezek gyakorlatilag jogosultságcsoportok, amelyeknek további konkrét elemeik is vannak, azaz ennél sokkal finomabban is szabályozhatunk, ha a következő képen látható, részletes mappa jogosultságokat használjuk.

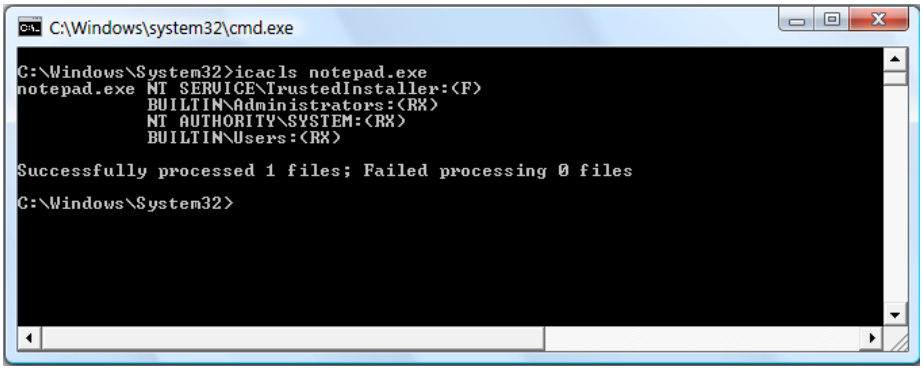
A fájlokkal kapcsolatban ugyanezeket az alapjogosultságokat kapjuk, azonban a jogosultságuk egyszerűbb, hiszen például egy Delete Subfolders and Files *(Almappák és fájlok törlése)* részletes jogosultságból csak az egyik rész lehet érvényes esetükben.



3.9. ábra: *A mappák részletes jogosultságai, illetve a hatókör lehetőségei*

Fájlrendszer jogosultságok kezelése a parancssorból

A jogosultságok parancssorból is kezelhetők, így igény szerint szkriptelhető és automatizálható is a folyamat. A Windows korábbi verzióiban használatos *cacls* (Change Access Control Lists) parancsot a Vistában a továbbfejlesztett, több lehetőséget nyújtó *icacls* váltja fel. Az elérhető paraméterek ismertetéséhez használjuk az *icacls /?* utasítást.



3.10. ábra: *A jogosultság kiosztó parancssori eszköz szintén univerzális*

Jogosultságkezelés alapok
Ebben a screencastban az operációs rendszer partíció, fájl- és mappa szintű hozzáféréseinek szabályzásáról lesz szó, részletes példákon keresztül.
Fájlnév: I-3-1a-Jogosultsagkezeles.avi

A hálózati megosztások jogosultságai

Ha egynél több számítógépet használunk egy szervezetben, már felmerülhet az igény bizonyos erőforrások, például a fájlok és a mappák közös használatára. A Windowsban lehetőség van ezeknek az erőforrásoknak a megosztására, így – megfelelő jogosultságok birtokában – távolról is egyszerűen elérhetjük őket. A megosztott objektumokat általában egy helyen, az első fejezetben bemutatott Computer Management MMC konzolból kezelhetjük, itt például felvehetünk, törölhetünk megosztásokat, illetve módosíthatjuk a meglévők biztonsági beállításait, de gyakorlatilag minden mappa tulajdonságai között is megtaláljuk ezt a lehetőséget [Share… *(Megosztás…)*].

A Windows Vistában további kétféle módon, varázslókkal is megoszthatunk mappákat: adott egy egyszerűsített megoldás, illetve a klasszikus változat is a rendelkezésünkre áll. Az, hogy melyiket kapjuk, azon múlik, hogy a vezérlőpulton a Folder Options *(Mappa beállításai)* alatt, a View *(Nézet)* fülön bekapcsolva hagytuk-e az alapértelmezett Sharing Wizardot *(Megosztás varázsló)*. Ha igen, akkor az egyszerűsített változattal is dolgozhatunk, ha nem akkor csak és kizárólag a klasszikussal.

A mappamegosztás engedélyezése esetén a számítógépünk egyből fájlkiszolgálóvá változik (azért nem úgy, mint egy valódi hálózati kiszolgáló operációs rendszer, részletekért lásd a 4. fejezetet) – míg a megosztáshoz kapcsolódó másik gépből ügyfél lesz. Fontos körülmény, hogy a mappamegosztásokat

nem az egyes felhasználók végzik (viszont csak az emelt szintű jogosultsággal rendelkező felhasználók indíthatják a megosztás folyamatát), hanem az operációs rendszer. Ez azért fontos, mert ennek megfelelően a hálózati megosztás eléréséhez elég a számítógép bekapcsolt állapota, nem szükséges egy-egy felhasználó interaktív belépése. Ebből az is következik, hogy a konfigurált megosztások a rendszer újraindítása után is megmaradnak és a következő alkalommal is elérhetőek lesznek.

A megosztások beállításához és működéséhez a File and Printer Sharing *(Fájl- és nyomtatómegosztás)* szolgáltatásnak engedélyezve kell lennie az adott hálózati profilban. Ezt a Network and Sharing Centerben *(Hálózati és megosztási központ)* tudjuk ellenőrizni.

Általában szükséges és elvárt lépés a megosztásokhoz jogosultságokat is kiosztani. Ez esetben mindenképpen hitelesítenie is kell magát az ügyfélgép felhasználójának. A mappamegosztásoknál alapvetően csak három jogosultsági szint létezik, amelyek az engedélyek szintje szempontjából gyakorlatilag teljesen megegyeznek az NTFS ugyanilyen nevű jogosultságaival:

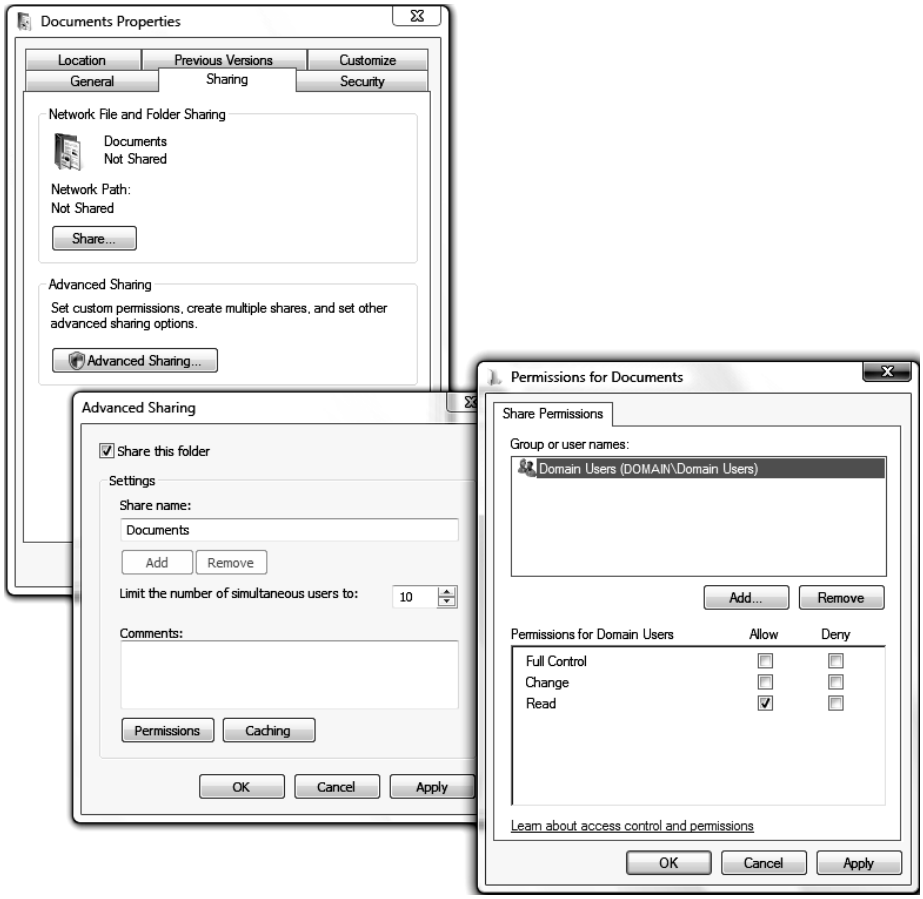
- Read *(csak olvasás),*
- Modify *(módosítás),*
- Full Control *(teljes hozzáférés).*

Fontos tudni azt is, hogy a helyi fájlrendszeren (NTFS) érvényes és a hálózati megosztásnál megadott jogosultságok közül – párhuzamosság esetén – mindig a szigorúbb, (más szóval a különböző jogosultságok metszete), lesz az érvényes, tehát ha az egyik ponton csak olvasást, a másikon pedig írást is engedélyezünk az objektumhoz, akkor csak olvasásra férhetünk majd hozzá.

Szemléltessük ezt egy példa segítségével: a *gtamas* felhasználó tagja a Users, illetve a HaladoUsers csoportnak is. A *D:\Temp* mappához emiatt aztán többféle NTFS-jogosultsága is van, illetve mivel ez egy megosztott mappa is egyben, és más gépről is el kell érnie, megosztási joggal is rendelkezik a csoporttagsága révén.

Felhasználó/ csoport	NTFS jogok	Megosztás jogok	Érvényes jog
gtamas	Full Control	Read	
Users	Modify	–	
HaladoUsers	Modify	Read	
Összegzés	**Full Control**	**Read**	**Read**

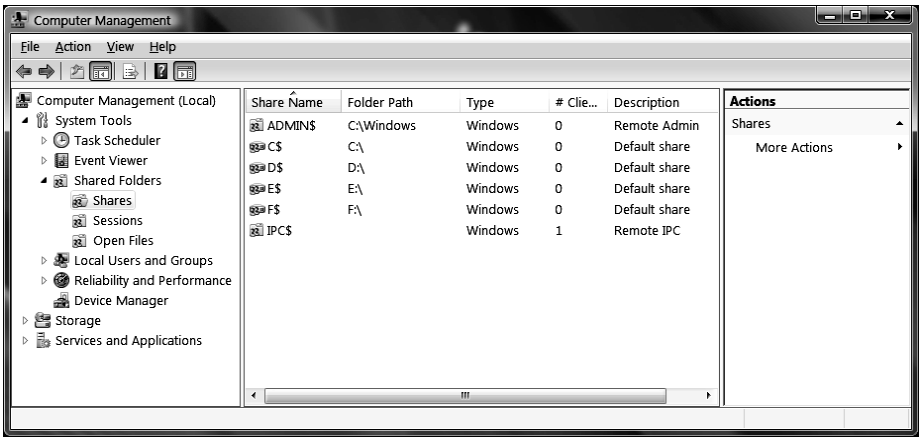
A megosztásokat a grafikus felhasználói felületen kívül parancssorból is kezelhetjük a *net* parancs *use* paraméterrel történő használatával. Az aktuális hálózati megosztások listájához csak egyszerűen, egyéb kapcsolók nélkül adjuk ki a *net use* utasítást.



3.11. ábra: *Jogosultságok a Windows Vista egy megosztott mappáján*

Speciális megosztások

A Windows operációs rendszerekben hagyományosan és alapértelmezés szerint léteznek speciális megosztások is, elsősorban a rendszergazdák munkájának könnyítése, illetve a számítógépek és alkalmazások egyszerűbb kommunikációja okából. Ezeket Default Administrative Shares-nek *(alapértelmezett felügyeleti megosztásoknak)* hívjuk, és a már többször említett Computer Management MMC-ben tekinthetjük meg ezek listáját, de a *net share* parancs is képes ugyanerre.



3.12. ábra: *Jogosultságok a Windows Vista egy megosztott mappáján*

Ezen megosztások közös jellemzője, hogy a nevük a $ karakterrel kezdődik, amely gyakorlatilag annyit jelent, hogy a gépünk hálózatból történő tallózásnál nem fognak látszani, csak direktben, közvetlenül a teljes megosztási név *(\\gép\megosztas$)* formájában lehet ezekre hivatkozni. Viszont mi magunk is hozhatunk létre a *$* jellel rejtett megosztásokat. Az is látható az ábrából, hogy mindegyik partíció rendelkezik alapértelmezés szerint, (anélkül, hogy megosztanánk), egy-egy ilyen megosztással. Ezen kívül a következő speciális mappák rejtett megosztások is egyben:

- ADMIN$: Az adott operációs rendszer rendszerkönyvtára, általában a *C:\Windows* mappa.
- IPC$: Hálózatban, a gépek közötti kommunikációt szolgáló megosztás *(Inter-Process Communication).*
- Print$: nyomtató esetén, a nyomtatómeghajtó program lelőhelye lesz ez a megosztás, általában a *C:\Windows\system32\spool\drivers* mappa.

Erőforrás-megosztás
Ebben a screencastban a Windows Vistával kivitelezhető erőforrás-megosztásról, azaz a fájl- és nyomtatókiszolgálókénti működés lehetőségeit mutatjuk be.
Fájlnév: I-3-1b-Eroforras-megosztas.avi

A megosztott nyomtatók jogosultságai

A Vistában természetesen van lehetőségünk a géphez illesztett nyomtatók megosztására, tipikusan egy másik felhasználó által, a hálózatból történő használatra. Ebben az esetben viszont szükséges lesz jogosultságokat meghatározni az adott nyomtató lehetőségeivel kapcsolatban. A fájlrendszer- vagy a megosztásjogosultságokkal összehasonlítva a nyomtatási jogosultságok lényegesen szűkebb körűek, gyakorlatilag az összeset tartalmazza a következő táblázat.

Jogosultság	Részletek
Print *(Nyomtatás)*	dokumentumok nyomtatása; saját dokumentumok nyomtatási jellemzőinek beállítás; saját dokumentumok nyomtatásának megállítása, újraindítása és törlése.
Manage Printers *(Nyomtatókezelés)*	a nyomtató megosztása; a nyomtató tulajdonságainak megváltoztatása; a nyomtató eltávolítása; a nyomtatási jogosultságok megváltoztatása; a nyomtató leállítása és újraindítása.
Manage Documents *(Dokumentumok kezelése)*	az összes – a nyomtatási sorban lévő – dokumentum nyomtatásának megállítása, újraindítása, mozgatása és törlése.

Ha megosztunk egy nyomtatót, akkor a jogosultsági listájába alapértelmezés szerint bekerül az Everyone csoport, a szimpla nyomtatás joggal, továbbá a jogosultsági listában szerepel még az Administrators csoport is, az összes elérhető nyomtatási jogosultsággal.

A felhasználói engedélyek

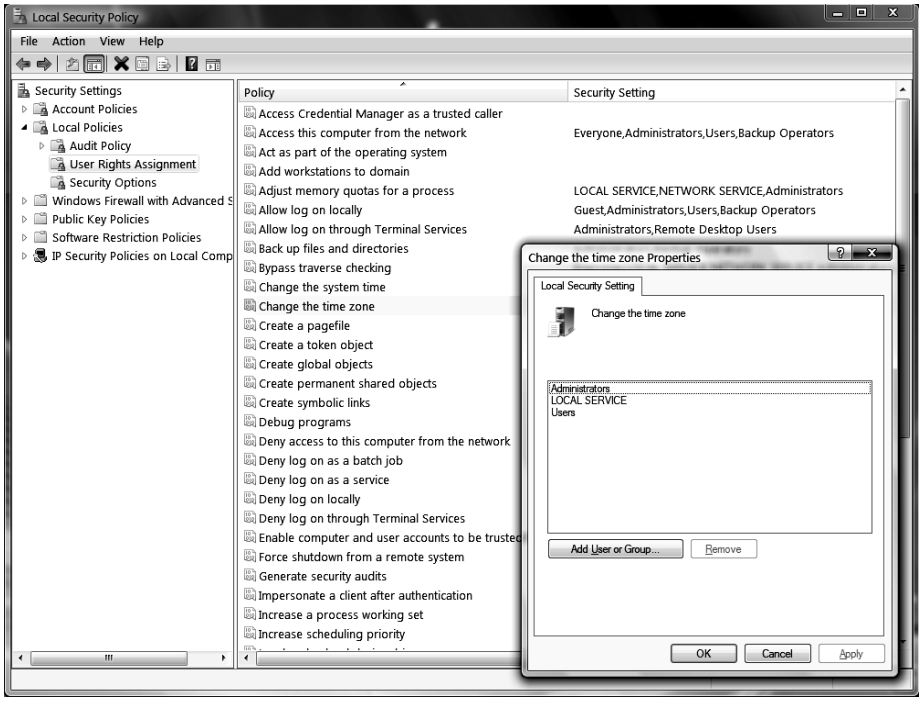
Ha szeretnénk tisztában lenni az erőforrás-kezelés témakörrel, akkor világosan kell látnunk, hogy a hitelesítést követő engedélyezés folyamata (autorizáció) nemcsak a sokkal inkább a szemünk előtt lévő fájl-, megosztás-, vagy pl. a nyomtatási jogosultságokra vonatkozhat, hanem az egész számítógépet érintő engedélyekre is. A különbség éppen a hatókör, azaz az engedélyek tárgya kö-

zött van, mert amíg a jogosultságok általában egy-egy objektumot érintenek, az engedélyek az operációs rendszer működésével kapcsolatosak, ráadásul többnyire eléggé komoly hatást kifejtve.

Ezen engedélyek meghatározása, illetve változtatása általunk is befolyásolható, még ha ezt általában tényleg csak indokolt esetben szükséges elvégezni. Ahhoz, hogy megtekinthessük a gépre vonatkozó engedély listát, indítsuk el a Local Security Policy *(Helyi biztonsági házirend)* MMC-konzolt.

Ezt az MMC-t csak a Business, Enterprise, vagy az Ultimate változatoknál érjük el, viszont ezeknél képesek vagyunk elindítani egyszerűen is: gépeljük be *Start/Run* mezőbe vagy a parancssorba a *secpol.msc* parancsot.

Ezután navigáljunk el a *Security Settings\Local Policies\User Rights Assignment (Biztonsági beállítások\Helyi házirend\Felhasználói jogok kiosztása)* pontra, ahol az összes opciót egy tetszetős, csoportosított listában, az MMC-konzol jobboldali keretében láthatjuk.



3.13. ábra: *Az engedélyeket a házirenden keresztül szabályozhatjuk*

Rögtön látható, hogy jó pár opció esetén már az alapbeállítás, azaz a megfelelő felhasználói fiókok, illetve a csoportok hozzárendelése megtörtént, ami azért logikus, mert pl. az Allow Log On Locally *(Helyi bejelentkezés engedélyezése)* engedély nélkül senki sem használhatná az operációs rendszert. Ha alaposan megnézzük a lista elemeit, akkor azt is észrevehetjük, hogy néhány esetben az engedélyek eleve tiltás formájában is szerepelnek, egy közös Deny (magyarul viszont több, különféle nyelvtani módszerrel megoldott) előtaggal:

- Deny Access This Computer From The Network (A számítógép hálózati elérésének megtagadása)
- Deny Allow Log On Through Terminal Services (Terminálszolgáltatások használatával történő bejelentkezés tiltása)
- Deny Log On As A Batch Job (Kötegelt munka bejelentkezésének megtagadása)
- Deny Log On As A Service (Szolgáltatáskénti bejelentkezés megtagadása)
- Deny Allow Log On Locally (Helyi bejelentkezés megtagadása)

Ezeknek az opcióknak mindig van tehát engedélyező változata is, azaz kétfajta módon is tudjuk finomhangolni a hozzájuk tartozó lehetőséget. Alapértelmezés szerint pl. a helyi belépés engedélyezve van a helyi Guest fióknak, illetve az Administrators, Backup Operators, és Users csoportoknak. Ha valamely felhasználótól szeretnénk elvenni a helyi belépés jogát – annak ellenére, hogy pl. a Users csoport tagjaként ez jár neki –, akkor a tiltó opció alá felvehetjük, konkrétan nevesítve a fiókját. Mivel az tiltás „erősebb" lehetőség, a felhasználó nem fog tudni belépni az operációs rendszerbe.

Ezen engedélyek kiosztása tehát a gyári beállításon alapul, de akár mi magunk is változtathatunk ezen a helyzeten, illetve a rendszer némiképp egy automatizmussal is színesíti lehetőségeket. Egy példa: ha hálózati megosztásokat engedélyezzük a Network and Sharing *Centerben (Hálózati és megosztási központ)*, és egyúttal a jelszóval védett hozzáférést kikapcsoljuk (lehetőleg ne tegyünk ilyet, ez csak egy példa), akkor a Guest fiók kikerül a korábban említett Deny Allow Log On Locally *(Helyi bejelentkezés megtagadása)* engedély opcióból.

Az engedélyek listája terjedelmes (kb. 45 db), értelmük és felhasználási területeik gyakran mély ismereteket igényelnek magáról az operációs rendszerről. Ennek a könyvnek nem szándéka az engedélyek egyenkénti alapos bemutatása, annyit viszont mindenképpen célszerű megjegyezni, hogy ha bármelyik opciót megnyitjuk, akkor az Explain *(Magyarázat)* fülön egy-egy frappáns értelmezést kaphatunk az adott engedély jelentéséről, illetve az esetleges verzió függőségekről is.

A magyarázatoknak a legtöbb esetben része a biztonsági felhívás is, amely szerint óvatosan bánjunk a gyári beállítások konfigurálásával vagy az esetleges törlésekkel, hiszen súlyos, esetleg visszaállíthatatlan sérüléseket is okozhatunk a nem átgondolt változtatásokkal.

Windows XP Service Pack 2 biztonsági változások

A „kényelem + biztonság mindig = 1" tétel miatt kompromisszumok nélküli biztonságról sohasem beszélhetünk. A Windows asztali operációs rendszerek esetén korábban – főként a kompatibilitás és az egyszerű, kényelmes használat okán – némiképp háttérbe szorult a biztonságosság. Hozzátartozik a visszatekintéshez persze az a tény is, hogy nem is kellett olyan mértékű veszélyeztetettséggel számolnunk, mint napjainkban, amikor például az internet révén, a rendszereinket szinte minden oldalról folyamatos támadások érik. A Windows XP 2001-es kiadását követően viszont egyre több problémát okozott a sérülékenységek, illetve a rendszerek elleni incidensek számának növekedése, egyre szükségszerűbbnek látszott az alapos és mélyre hatoló korrekció. A Microsoft ekkor megtette az első szükséges lépéseket annak érdekében, hogy a számítógépes munkakörnyezet ebben az új, veszélyesebb világban is biztonságos és stabil legyen, akár az ügyfél oldali, akár a kiszolgáló oldali operációs rendszerekre gondolunk. Mi most az ügyféloldalra fókuszálva, az XP SP2 változásairól szeretnénk ebben a részben némi ízelítőt adni.

A redmondi szoftverfejlesztők új stratégiája, az úgynevezett Trustworthy Computing *(megbízható számítástechnika)* jegyében végül 2004 augusztusában megjelent a Windows XP második javítócsomagja, a Service Pack 2, mely szinte kizárólag a biztonságról szólt és több olyan újítást is bevezetett, melynek köszönhetően szinte újjászületett a rendszer. A megújult Windows tűzfal például alapértelmezésként bekapcsolásra került, az Internet Explorer pedig – mely mindig is központi téma volt, ha Windows-biztonságról esett szó – az előugró ablakok blokkolásával és a különböző letölthető beépülő modulok továbbfejlesztett kezelésével jeleskedett. A rendszerben az egyre gyakoribbá váló puffer-túlcsordításos támadások elleni védelemként bevezetésre került a Data Execution Prevention (DEP/NX), mely az operatív tár védelmét hivatott szolgálni oly módon, hogy az adatok számára fenntartott memóriacímeken tiltja a kódvégrehajtást. További újdonság volt még a DCOM-rendszerkomponensek és az azokat koordináló RPC-szolgáltatás (távoli művelet végrehajtás) biztonsági szintjeinek emelése.

3.14. ábra: *Security Center*

A felhasználói felületen nem sok minden változott, az egyetlen szembe tűnő újdonság a Security Center *(Biztonsági központ)* megjelenése volt, mely a Windows beépített és a külső fejlesztők által telepített biztonsági szolgáltatások (tűzfal, antivírus, automatikus frissítések) állapotát felügyeli.

Könyvünkben a Windows XP SP2-ben megjelent Security Center bemutatása a Vista Security Centerrel együtt történik meg, a következő alfejezetben.

Újdonságok a Vista biztonsági rendszerében

A Microsoft a Windows Vista készítésének idejére már teljesen új alapokra fektette szoftverfejlesztési stratégiáját, azaz a biztonság – nagyon előkelő helyen – bekerült az elsődleges szempontok közé. Ennek megfelelően az új operációs rendszer soha nem látott technológiaarzenált vonultat fel, melyek mind-mind a rendszer és az adatok védelmét szolgálják. A következőkben a Windows Vista biztonsági szolgáltatásait ismertetjük, az alapoktól egészen a felhasználók számára is tapasztalható megoldásokig.

Védekezés a mélyben

Ebben a részben a Windows Vista olyan felszín alatti, gyakran általunk nem is befolyásolható, beállítható komponenseinek és szolgáltatásainak az áttekintését kíséreljük meg, amelyek majdnem 100%-osan újdonságnak számítanak. Úgy gondoljuk, hogy függetlenül attól, hogy a napi szintű üzemeltetésben nem találkozunk konkrétan ezekkel a megoldásokkal – hanem általában csak maximum az előnyeiket élvezzük –, tájékozottnak kell lennünk a biztonságos működés megteremtésének minden részletével. Ennek megfelelően a jelen fejezetbe a *programkód*, a *kernel*, a *rendszerfájlok*, és a *memória* védelmével, sérthetetlenségével és működési specialitásaival kapcsolatos tudnivalókat szerkesztettük össze.

A programkód integritásának védelme

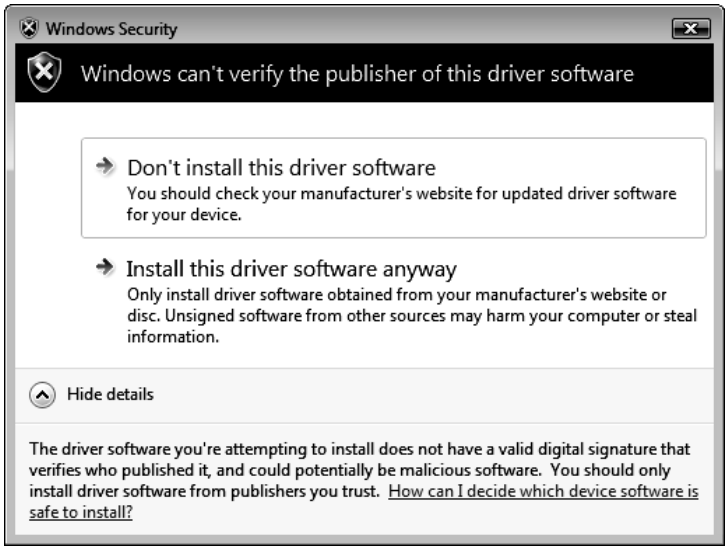
A Windows rendszerfájlok védelme az illetéktelen módosítások és cserék ellen alapvető fontosságú a rendszer stabilitása és megbízhatósága szempontjából. A rendszerkomponensek védelmére már a korábbi verziókban is volt eszköz (System File Checker, SFC), a Windows Vista azonban már a rendszerbetöltő és a kernel szintjén tartalmaz egy szolgáltatást, mely a kritikus rendszerfájlok kód-aláírását ellenőrzi.

A 64-bites operációs rendszerek támogatása apropóján új hardverek, új eszközmeghajtók, és új alkalmazások jelennek meg, ezért a Microsoft számos új – a kompatibilitás megőrzése miatt eddig megvalósíthatatlan – megoldást épít be 64-bites termékeibe, melyek így végre „tiszta lappal”, az alapoktól kezdve biztonságosként épülhetnek meg.

A Windows Vista 64-bites támogatása az x64-es rendszerek esetben értendő, Itaniumra készült változatot a Microsoft nem adott ki. A 64-bites operációs rendszerekről részletesebb információt a következő TechNet Magazin cikkből érhetünk el: http://download.microsoft.com/download/a/1/a/a1ac3b96-011e-4cca-9dba-78973187567d/26-29.pdf vagy http://tinyurl.com/2q22jz

A 32-bites világgal egyelőre természetesen fenn kell tartani a kompatibilitást, a kód integritás védelem így a 32- és a 64-bites platformokon némiképp eltérően működik.

- **x64**
  - Minden kernelmódban futó kódot digitális aláírással kell ellátni. Ez biztosítja, hogy a fájl bizonyíthatóan a saját kiadójától származzon. Ha a komponens nincs aláírva, a Windows megtagadja az állomány futtatását.
  - A külső kódoknak – illesztőprogramok, segédalkalmazások stb. – WHQL-kompatibilitási és minőségi, illetve Microsoft Certificate Authority tanúsítvánnyal kell rendelkezniük. Ez alól semmilyen program nem lehet kivétel.
- **x86**
  - A kompatibilitás fenntartása érdekében a 64-bites platformhoz képest több kompromisszumra is kényszerült a Microsoft. A digitális aláírást csak illesztőprogramok esetén ellenőrzi a rendszer, de ha a kód nem rendelkezik ilyennel, a Windows akkor is engedélyezheti a telepítést, ami házirend, vagy beállításfüggő opció is lehet, tehát egy vállalati hálózatban megkövetelhetjük a csoportházirenden keresztül a kötelező aláírást. A Microsoft által szállított, beépített eszközmeghajtók természetesen mind rendelkeznek aláírással.
  - Az alkalmazásszinten futó programoknál nem követelmény sem a digitális aláírás, sem a WHQL-tanúsítvány, ez azonban szintén a biztonsági házirendből szabályozható, tehát a rendszergazda opcionálisan engedélyezheti a védelmet.



3.15. ábra: *Figyelemfelhívás eszközmeghajtó telepítéskor*

A Vista rendszervédelem

A Vista Windows Resource Protection (WRP) megoldását sokszor a korábbi Windows File Protection (WFP) megoldással azonosítják. A WFP a Windows 2000-rel és egy hasonló megoldás, a System File Protection (SFP) pedig a Windows Millennium Editionel lett bevezetve. Mindkettő hasonlít a WRP-re de szignifikáns eltérések vannak a megvalósításban.

A WFP csak fájlokat figyel, míg a WRP a kritikus fájlokat, mappákat és a regisztrációs adatbázis bejegyzéseit is védi. A WFP/SFP csak a védett rendszerfájlokat érintő módosításokat figyeli. Amennyiben ezek a változások nem hitelesítettek, a WFP/SFP visszacseréli a módosult állományokat egy korábbi megbízható mentésből. A leggyakoribb figyelmeztetés, amit a WFP korábban adott, egy felhasználói figyelmeztetés, vagy egy eseménynapló-bejegyzés volt.

A WRP tovább erősíti a rendszererőforrások védelmét, kiterjesztve a védelmet a regisztrációs adatbázisra és rendszermappákra is. A Vista esetében a Rendszergazdák *(Administrators)* csoport tagjai sem módosíthatják a rendszererőforrásokat. Alapértelmezés szerint csak a Windows Trusted Installer security principal jogosult módosításokra a Windows Module Installer szolgáltatáson keresztül. Ezt használja a Windows Installer, a *hotfix.exe*, és az *update.exe* is.

A rendszergazdáknak azonban jogukban áll módosítani és tulajdonba venni a védett rendszererőforrásokat is, és teljes jogot adniuk maguknak, így módosítani vagy törölni is rendszer számára kritikus állományokat. A WFP-vel ellentétben a WRP viszont nem állítja helyre automatikusan a védett állományokat megbízható mentésből, csak újraindítás során állítja vissza a rendszer indulásához szükséges állapotot.

Ahhoz, hogy a WRP visszaállítsa az összes védett erőforrást (ami hasznos lehet egy hibakeresés során) futtassuk a következő parancsot: *sfc /scan now*. A védett fájlok eredeti állapotának visszaállításához szükséges lehet a Vista telepítőmédia is.

Kernel-patch Protection (PatchGuard)

A kernel, vagyis a rendszermag a legalacsonyabb szintű komponense az operációs rendszernek. A rendszerindítási folyamat során elsőként töltődik be, majd olyan feladatokat lát el, mint a programok indítása, memória-, és a fájlrendszer kezelése. A kernel teszi lehetővé, hogy az egyes alkalmazások „beszélgethessenek" a hardvereszközökkel, így a mag sebessége és megbízhatósága alapvető fontosságú a rendszer egészére nézve.

A kernel külső eszközökkel történő módosításával szükségszerűen megbomlik a mag integritása, ami kihatással lehet a Windows stabilitására, de akár biztonságára is. A különböző védelmi programok (antivírusok, antispyware alkalmazások) gyártói a múltban gyakran alkalmazták ezt az eljárást, hogy elejét vegyék egy-egy fertőzésnek azáltal, hogy közvetlenül kernelszinten akadályozták meg egyes ártalmas programoknak, hogy bizonyos rendszerfüggvényeket hívjanak meg. Sajnos azonban nemcsak az antivírus cégek alkalmazták a kernelmódosítást, hanem a különböző vírusokat készítő programozók is, hiszen ilyen módon akár a fájlkezelők elől is elrejtőzni képes, úgynevezett rootkiteket is bejuttathattak a rendszerbe, amelyek aztán szabadon garázdálkodhattak, anélkül, hogy bármely védelmi program tudomást szerzett volna jelenlétükről.

A kernelmódosítás elleni védelem nem újkeletű, először a Windows XP és a Windows Server 2003 64-bites változataiban találkozhattunk vele az x64-es AMD64 és Intel EM64T processzorok bevezetésének ideje körül. A 64-bites Windows Vistában azonban megkerülhetetlen lett a technológia – amint a Windows jogosulatlan kernelmódosítást érzékel, automatikusan leállítja a rendszert.

Azért, hogy a biztonságtechnikai cégek különböző védelmi programjai a továbbiakban is együttműködhessenek a rendszerrel, a Microsoft olyan további technológiákat bocsát a cégek rendelkezésére, melyekkel a kernel módosítása nélkül is megfelelő kiegészítő védelemmel láthatják el a felhasználókat:

- **Windows Filtering Platform** *(Windows szűrőplatform)* – olyan hálózati műveletek engedélyezése, mint a csomagelemzés, például harmadik féltől származó tűzfal működésének támogatásához.
- **File System Mini Filter** – programok hozzáférésének biztosítása a fájlrendszer-műveletek figyeléséhez.
- **Registry Notification Hooking** – a Windows XP-ben bemutatott, de a Vistában továbbfejlesztett eljárás, mely lehetővé teszi a programoknak, hogy valós időben kövessék a rendszerleíró-adatbázis módosulásait.

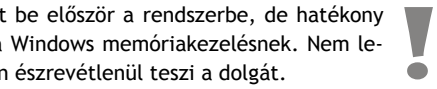
Address Space Layout Randomization (ASLR)

Az Address Space Layout Randomization hasznos rendszerszintű újítás a Windows Vistában. A technológia lényegében egy memóriavédelmi megoldás, mely azáltal, hogy véletlenszerűen megkeveri a memóriacímeket, nagyban megnehezíti a káros programok működését.

Az eljárás lényege, hogy a Windows egy-egy program vagy folyamat kulcsterületeit (futó kód, könyvtárak, heap, vermek stb.) minden alkalommal véletlenszerűen meghatározott memóriacímekre tölti be, ellentétben a régebbi, ASLR nélküli eljárással, amikor a rendszerfüggvények minden esetben ugyanarra a memóriacímre kerültek, tehát közismertté vált a tartózkodási helyük. Ha egy vírus káros kódot szándékozik injektálni a memóriába, először megpróbál meghívni egy rendszerfüggvényt, majd vár ennek a függvénynek a visszatérési értékére. Mivel az ASLR véletlenszerűen (és külön-külön) mozgatja a függvényeket a memóriában – egészen pontosan 256 különböző helyre töltheti be őket minden egyes alkalommal –, a vírusnak 1/256-od esélye van, hogy éppen eltalálja azt a memóriacímet, ahol a kiszemelt érték tartózkodni fog. Ez a technika megnehezíti egy lehetséges külső támadó dolgát, mert egyrészt nem jósolható meg előre a konkrét memóriacím, másrészt a kiszámítása (helyesebben próbálgatása) sem túlságosan kifizetődő módszer. Az ASLR hatóköre a következőkre terjed ki:

- visszatérési verem;
- heap- (vagy halom-) memória;
- az operációs rendszer részeként települő összes bináris állomány.

Az ASLR viszonylag későn, a Beta 2-es verzióban került be először a rendszerbe, de hatékony védelemnek bizonyult, így végül szerves részévé vált a Windows memóriakezelésnek. Nem lehet kikapcsolni, de engedélyezni sem kell – a háttérben észrevétlenül teszi a dolgát.



Az alábbi ábra néhány rendszerkomponens memóriában történő elhelyezkedését mutatja két indítási folyamat után.

- user32.dll (0x779b0000)
- kernel32.dll (0x77c10000)
- gdi32.dll (0x77a50000)

- user32.dll (0x770f0000)
- kernel32.dll (0x77350000)
- gdi32.dll (0x77190000)

Data Execution Prevention (DEP/NX)

A helytelen memóriahasználat azt jelenti, hogy valamilyen program egy nem futtatható kódot tartalmazó memóriaterületet erővel kódfuttatásra akar használni. Tipikusan ilyenek azok a rosszindulatú programok, amelyek egy esetleges puffer-túlcsordulásos sérülékenységet kihasználva tárolnak le futtatható gépi utasítások sorozataként értelmezhető adatokat (=program) verem-, adat-, heap- stb. területként kijelölt memóriába, majd az így betöltött kódnak adják át a vezérlést.

A DEP úgy védekezik az effajta támadások ellen, hogy az adatszegmensek számára fenntartott memóriacímeket *nem futtatható*-ként jelöli meg, így ezekről a területekről nem indítható kód. A DEP működéséhez vagy operációsrendszer- vagy processzorszintű támogatás szükséges, így beszélhetünk hardveres, illetve szoftveres DEP-ről is.

- **Hardveres DEP** – A legtöbb ma kapható processzor (az összes 64-bites CPU, valamint egyes 32-bites Intel és AMD processzorok is) már rendelkezik ezzel a képességgel. Az erre alkalmas processzorok a memória kezelésekor belsőleg használt lapozótábla-bejegyzések utolsó bitjét NX (No eXecute) mutatóként értelmezik: 0 esetén a hivatkozott területen lehetséges, 1 értéknél tilos a kód futtatása. (Megjegyzendő, hogy az NX az eredeti AMD-s elnevezés, az Intel terminológiájában XD bitről – eXecute Disable – beszélünk.)
- **Szoftveres DEP** – A DEP NX vagy XD bittől független, szoftveres megvalósítása kicsit bonyolultabb, de nem lehetetlen. Az eljárás neve – Safe Structured Exception Handling (SafeSEH), vagyis biztonságos *struktúrájú kivételkezelés* – már mutatja, hogy a memóriavédelem ez esetben a Windows kivételkezelő mechanizmusán keresztül valósul meg. A SafeSEH követelményeinek eleget tevő programoknak futtatáskor regisztrálniuk kell saját kivételkezelő eljárásukat. Régebbi, a DEP-et nem támogató alkalmazások használatakor a rendszer a kivételnek megfelelő funkció hívása előtt megvizsgálja: maga a kivételkezelő kód futtatható memóriaterületen van-e.

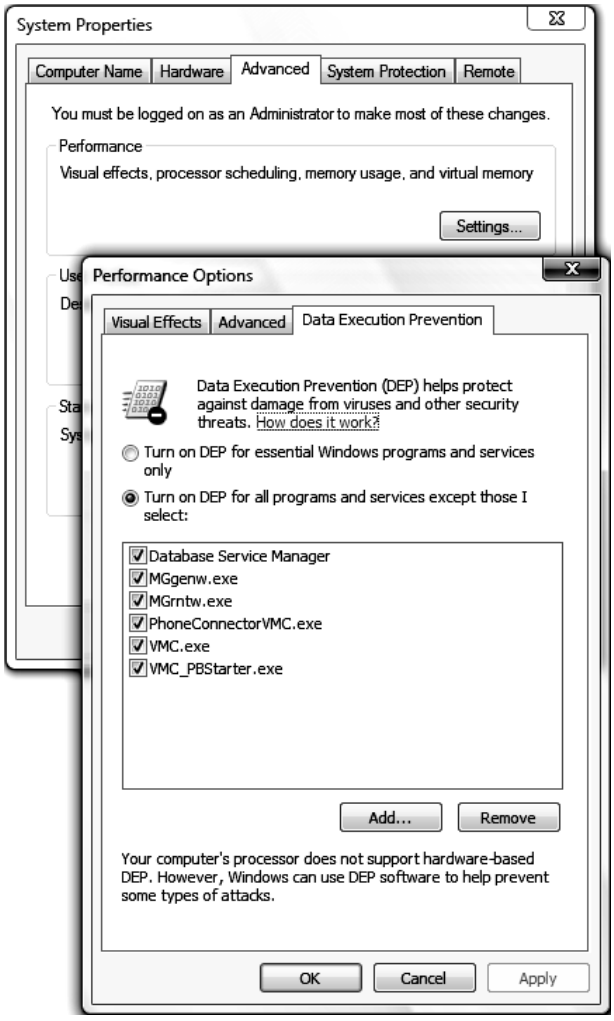
Akár hardveres, akár szoftveres DEP-ről van szó, a rendszer nem javítja ki például a puffer-túlcsordulásos sérülékenységeket, és nem akadályozza meg memóriaterületek felülírását. Amikor azonban a vezérlés adatterületre kerülne, akkor vagy hardveres kivétel generálódik, vagy a kivételgenerálást az operációs rendszer szoftveres úton végzi el, mely során az ártó kódok lefülelhetők.

A DEP beállításait Windows XP, illetve Windows Server 2003 esetében a rendszerbetöltés indításáért felelős *boot.ini* konfigurációs fájlban határozhatjuk meg, mely a rendszerpartíció gyökérkönyvtárában foglal helyet. Az operációs rendszer bejegyzésének végén található */noexecute* kapcsolónak négy állása van: *AlwaysOn, AlwaysOff, OptIn* és *OptOut*.

- AlwaysOn – A DEP engedélyezve van, kivétel nélkül minden futtatható állományra.
- AlwaysOff – A DEP le van tiltva.
- OptIn – A DEP csak a Windows saját futtatható állományaira vonatkozik. Ez az alapértelmezett beállítás.

- OptOut – A DEP minden futtatható állományt felügyelete alatt tart, de a rendszergazdák a *Control Panel/System/Performance* lapján kivételeket képezhetnek a memóriavédelmi eljárás hatóköre alól.

A felsorolt kapcsolók mindegyike érvényesül hardveres és szoftveres DEP-nél egyaránt. A rendszer a *boot.ini*-be írt explicit */noexecute= OptIn* kapcsolóval települ, illetve amennyiben a *boot.ini*-ből valamilyen okból eltávolítják a */noexecute* kapcsolót, akkor a Windows úgy viselkedik, mint ha a */noexecute=OptIn* lenne érvényben.



3.16. ábra: *Akcióban a DEP, a lista szereplői pedig a kivételek a hatása alól*

Mivel a Windows Vista már nem használja a *boot.ini* állományt, (sem az NTLDR rendszerbetöltőt), az új Boot Configuration Data (BCD) szerkesztésével konfigurálhatjuk a DEP-et. Ehhez használjuk a beépített *bcdedit* parancsot, mely paraméterek nélkül tájékoztatást ad a DEP pillanatnyi állapotáról.

A DEP *bcdedit*-tel történő beállításához a következő parancsokat használhatjuk (a paraméterek jelentése megegyezik a korábbiakkal):

- bcdedit /set nx OptIn
- bcdedit /set nx OpOut
- bcdedit /set nx AlwaysOn
- bcdedit /set nx AlwaysOff

A szolgáltatások megerősítése: Service hardening

A Windows szolgáltatások kedvelt támadási célpontjai a különböző vírusoknak és egyéb kártevő programoknak, mert ezek a folyamatok többnyire rendszerjogosultsági szinten futnak, tehát lényegében bármihez korlátozás nélkül hozzáférhetnek. A Vista ezen a téren is újít, a szolgáltatások zöme immár nem a *LocalSystem* fiók nevében fut, így nincs is teljhatalma a rendszer fölött.

Néhány szó a szolgáltatásfiókokról

A szolgáltatásfiókok előre definiált hozzáférési lehetőségek a Windows beépített szolgáltatásainak futtatásához. A Windows Vista három ilyen fiókkal rendelkezik (miként a korábbi operációs rendszerek is).

A „legerősebb" ún. *LocalSystem* fiók nem rendelkezik jelszóval, mégis teljes hozzáférése van a rendszer egészéhez, magában foglalja a beépített Administrators *(Rendszergazdák)* csoport jogosultsági körét is, hálózati környezetben pedig ez a szolgáltatás testesíti meg magát a „számítógépet", tehát a hálózati hitelesítés is ezen a fiókon keresztül történhet.

A szolgáltatások korábban szinte kivétel nélkül a *LocalSystem* fiók használatával futottak, így sokszor szükségtelen jogosultságokat kaptak, ami az előbb leírtakat figyelembe véve komoly biztonsági aggályokat vethet fel. A Windows Vistában az XP-hez képest a szolgáltatások töredéke fut helyi rendszerfiókkal, a többségük átkerült a csökkentett jogosultságokkal rendelkező *LocalService*, illetve *NetworkService* fiókokba.

Viszont a szolgáltatás működéséhez néha azért elengedhetetlenül szükséges, hogy rendszerjogosultságokat élvezzen, ezért a Microsoft programozói egy trükköt vetettek be: ezeket a szolgáltatásokat egyszerűen „kettévágták", és a kódnak csak a privilegizált műveleteket végző része fut a *LocalSystem* fiók

alól, a többi továbbra is a *LocalService* hatókörében marad. A biztonság további fokozása érdekében a megosztott szolgáltatások két része közötti kapcsolathoz hitelesítés szükséges.

Emellett a szolgáltatások a felhasználókhoz hasonlóan saját egyedi biztonsági azonosítót kaptak, melyek az alábbi formátumban tárolódnak:

S-1-80-<a szerviz logikai nevének SHA-1 hash-e>.

Szintén a felhasználókhoz hasonlóan az egyes szolgáltatásoknak is csak adott műveletekhez van jogosultságuk. Ezeket a privilégiumokat a Registry tárolja, a *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services* kulcs alatt, a *RequiredPrivileges* értékben. A szolgáltatásfiókokhoz természetesen ACL is tartozik, így minden egyes szolgáltatásnak gondosan kijelölt munkaterülete van, melyen kívül nem tevékenykedhet, így még ha egy esetleges vírustámadás során a kártevő kód át is venné az irányítást a szolgáltatás fölött, akkor sem okozhat helyrehozhatatlan kárt. A szolgáltatások számára biztosított privilégiumok megfelelően kordában tartják a folyamatokat, korlátozzák a fájlrendszer és a registry használatát, valamint a Windows tűzfal által a hálózati kommunikációt is.

Hogy egy gyors példával demonstráljuk az új szolgáltatáskorlátozás jelentőségét, tekintsünk kicsit vissza az időben, 2003 augusztusára, amikor a *Blaster/Sasser* féregvírus globális problémákat okozott a Windows vehemens támadásával. A *Blaster* a rendszer egyik alapvető szolgáltatását, a Remote Procedure Call (RPC – *távoli eljáráshívás)* kerítette hatalmába, és a Windows folytonos újraindításával okozott fejfájást a felhasználóknak. A féreg ma már szinte semmilyen kárt nem tudna okozni, mert a Windows Vistában az RPC-szolgáltatás is átesett a fenti változásokon így:

- nem cserélhet le rendszerfájlokat,
- nem módosíthatja a registryt,
- nem befolyásolhat más szolgáltatásokat, és nem módosíthatja azok beállításait (például antivírus szoftverekét).

A szolgáltatások biztonsági konfigurálása a Windows telepítése során automatikusan megtörténik, azonban csak a rendszer saját beépített összetevőire érvényes, a külső és utólag telepített szolgáltatásokra nem.

Service Hardening
A rendszerszolgáltatások megerősítése fontos pont a Vista biztonságosságával kapcsolatban. Ebben a mini előadásban ezzel kapcsolatban mutatunk be részleteket.
Fájlnév: I-3-3a-Service-Hardening.avi

Változások a felhasználó fiókok és csoportok kezelésében

Ezen a területen az egyik legfontosabb változás a beépített Administrator *(Rendszergazda)* azaz a helyben egyetlen 500-as RID-del (a SID utolsó blokkja, 3-4 számjegy, normál felhasználók/csoportok esetén 1000-sel kezdődik) rendelkező fiók letiltása. Erre azért volt szükség, mert a gondatlanabb felhasználók és rendszergazdák a Windows telepítésnél általában nagyon gyenge jelszóval (pl. *123456*, *password*) látták el ezt a fiókot, vagy egyszerűen nem is adtak meg jelszót. A tiltás viszont passzol a Vista biztonsági modellhez, mert például egyrészt az UAC (lásd következő alfejezet) hatása nem terjed ki erre a fiókra, másrészt a hétköznapi munkára ne használjuk ezt a fiókot, mert nem erre való, ahogyan más rendszerekben sem.

Viszont néha mégiscsak szükségünk lehet erre a fiókra is, de ha le van tiltva, akkor hogyan érjük el? Mindig le van tiltva? Nem, speciális körülmények között, három esetben biztosan megkapjuk majd automatikusan az Administrator fiókot:

1. Csökkentett mód.
2. Startup Repair mód (a Vista DVD-ről indítva a rendszert).
3. Frissítő telepítés után (pl. XP > Vista).

Viszont mindegyik esetben csak és kizárólag akkor „él" automatikusan ez a fiók, ha nincs egy másik, a helyi Administrators csoportba tartozó fiók is a rendszerben, akár tartományban van a gép fiókja, akár nem.

Ide tartozik még az az újdonság is, hogy amennyiben egy új fiókot hozunk létre a rendszerben, az alapértelmezésként korlátozott felhasználói jogosultságokat kap.

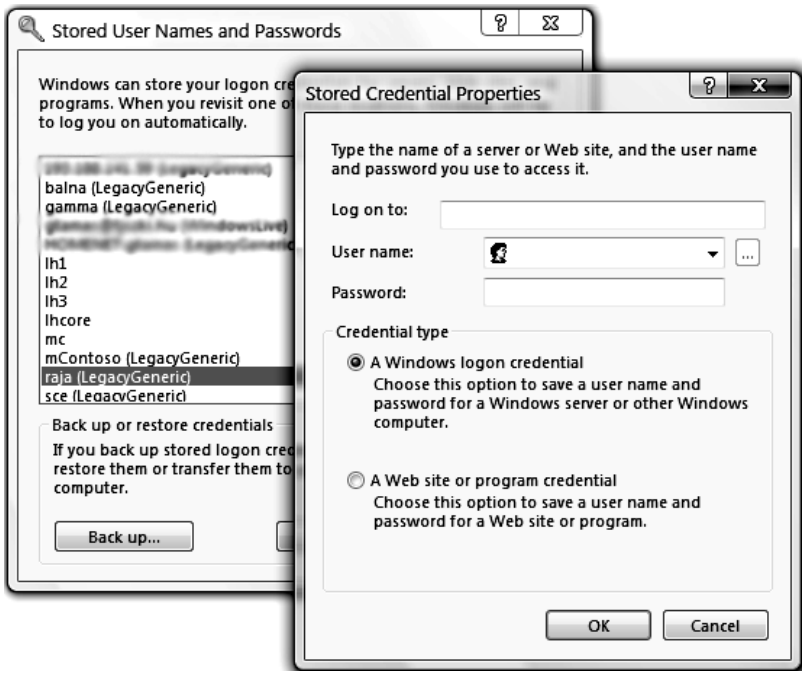
A felhasználói fiókokat érintő változások közül meg kell említenünk a korábbi a Windows XP-ben okban alapértelmezés szerint jelenlévő *Support* és a *Help* fiókok megszüntetése.

A csoportokról szólva, a legnagyobb változás a Power Users *(Kiemelt felhasználók)* csoport hatóköre gyakorlatilag megszűnt. Mivel a nevével ellentétben megtévesztően sok jogosultsággal rendelkeztek ennek a csoportnak a tagjai, így a rendszergazdák előszeretettel osztogattak efféle jogköröket a felhasználóknak – sok esetben teljesen feleslegesen. Két működő jogosultsági szint maradt tehát: Standard felhasználók (Users csoport), és a Rendszergazdák *(Administrators)* csoport.

Ezen kívül, a változó igényeknek megfelelően új csoportjaink is vannak, lássunk néhány példát:

- Cryptographic Operators: a PKI-val, IPSec-kel kapcsolatos feladatok jogosultságainak birtokosai.
- Distributed COM users: jogosultság az elosztott COM-objektumok eléréséhez, kezeléséhez.
- Event Log Readers: A csoport tagjai megnézhetik az Eseménynapló bejegyzéseit.
- IIS_IUSRS: lecseréli a korábbi IUSR_<gépnév> fiókot, azaz az anonim, webkiszolgálóhoz intézett kérések fiókjával egyenértékű, annak ellenére, hogy egy csoportról van szó.
- Performance log / Performance monitor users: a nevéből adódóan a Performance Monitor használatához kaphatnak (nem teljes körű) jogosultságot az e csoportba bekerülő felhasználók.

Tárolt hálózati nevek és jelszavak



3.17. ábra: *A jelszókezelő eszköz lényegesen komfortosabb lett*

A Windows Vista képes a hálózatban, valamint a weboldalakon használt jelszavaink tárolására. Ezt már a Windows XP-vel is megvalósíthattuk, de sokkal kevésbé komfortosan. A Vistával könnyedén előkészíthetjük a felhasználók számára például az intranetes szolgáltatások használatához szükséges belépési hitelesítő adatokat, és elmenthetjük ezeket.

Szükség szerint az esetleg tévesen bevitt hitelesítési információkat is törölhetjük, illetve teljes újdonságként a jelszavainkat el is menthetjük *.crd* kiterjesztéssel. A jelszavak tárolásának és beállításainak eléréséhez navigáljunk el a *Control Panel / User Accounts / Manage your network passwords* pontra.

A felhasználói fiókok felügyelete (UAC)

Egyértelműen belátható, hogy nemcsak a korábban említett rendszerszolgáltatások, hanem a rendszer interaktív felhasználói, azaz mi magunk is rendszeresen szükségtelenül magas jogosultsággal dolgoztunk a korábbi ügyfél operációs rendszereken. Ezért Vista esetén a Microsoft drasztikus változtatásokra szánta el magát ezen a területen is. Az új működési elv tömören: **mindenki standard felhasználó jogosultságú, senki sem rendszergazda, még akkor sem, ha annak látszik!** Ez az állítás elsőre bizonyára kissé meghökkentőnek tűnik, de a gyakorlatban működik, nézzük tehát lépésről lépésre a kiváltó okokat és a változásokat.

1. A régebbi rendszerekben a létrehozott felhasználói fiókok alapértelmezésként rendszergazdai jogosultságot kaptak, kezdve a telepítéskor létrehozott saját felhasználói fiókkal. Így a tapasztalatlan felhasználók kezében már a kezdetektől könnyen (ön)veszélyes fegyverré válhatott az operációs rendszer.
2. A Windows korábbi verzióival szerzett tapasztalatok azt mutatják, hogy a legtöbb olyan felhasználó, aki egyedül felügyeli számítógépét, mindenképpen rendszergazda-jogosultságú fiókkal használja azt, és nem sokat törődik a biztonsági figyelmeztetésekkel. Az ideális állapot természetesen az lenne, ha mindenki korlátozott felhasználóként lépne be a Windowsba, majd rendszerbeállítás módosításakor, vagy program telepítésekor átjelentkezne a rendszergazda fiókba, vagy a Run as… *(Futtatás mint...)* opciót használná. Az igazság azonban az, hogy jóval kényelmesebb eleve rendszergazdaként működtetni a rendszert, mert így szinte sosem fogunk ellenállásba ütközni.

3. Egy szigorú vállalati hálózatban is előfordulhat az, hogy egy ügyfélgépen jogosultságkezelési szempontból rosszul megírt, de kötelezően használt alkalmazás miatt muszáj a felhasználókat szükségtelenül magas szintű jogosultsággal ellátni, amely általában úgy zajlik, hogy a rendszergazda a helyi Administrators *(Rendszergazdák)* vagy a korábban említett, szintén túlságosan „erős" Kiemelt felhasználók *(Power Users)* csoportba beemeli a felhasználót.

Ezen helyzetek kiváltó oka egyrészt a tudatlanság, viszont másrészt a kényelem, amely ugyan szintén fontos szempont, de tudnunk kell azt is, hogy a rendszergazda-jogosultság teljes hozzáférést ad az operációs rendszerhez és a számítógép minden komponenséhez, lehetővé téve olyan módosításokat, amelyek a rendszert működésképtelenné tehetik, vagy kárt tehetnek más felhasználók adataiban. Sőt, az óvatlan használattal a kívülről érkező kártevők, vírusok, férgek, spyware-ek sem ütköznek túl sok akadályba – hiszen, amint bejutnak a gépre, rögtön rendszergazda-jogosultságot szerezhetnek. Valamint, üzemeltetőként azt a tényt is célszerű ismernünk, hogy a rendszereket érintő biztonsági incidensek közel 70%-a a belső hálózat felhasználóitól származik. Ezek ismeretében bizonyára el fogunk gondolkozni azon, hogy megéri-e az emelt szintű jogosultsági vakmerő használata.

A Vistában viszont nem kell sokat ezen gondolkoznunk, alapértelmezés szerint kész helyzet elé vagyunk állítva, amely talán kevésbé kényelmes, viszont annál hasznosabb. A kész helyzet szállítója az ún. User Account Control (UAC, *Felhasználói fiókok felügyelete),* amely egy összetett megoldás, ez a következő alfejezetek közül több is ennek a technológiának a részletezésével foglalkozik majd.

Ha például a mindennapos használat közben adunk hozzá felhasználókat, akkor azok immár csak a standard felhasználói jogokkal bírnak majd. Ha a telepítéskor elsőként létrejövő fiókot nézzük, az természetesen továbbra is rendszergazda-jogosultságú lesz, de neki is – mind minden a helyi rendszergazdacsoportba tartozó fióknak – csökkentett, standard felhasználó szintű környezetet tölt be a Windows, a rendszermódosításhoz szükséges jogokat külön kell kérnie.

Egy szó mint száz, alapesetben a jogosultságok túlzó kiosztása miatt kevesebbet kell aggódnunk, de mi a helyzet akkor, ha mégis szükség van rendszergazdaként működtetni a gépet. Mert ugyan az is fontos és kissé talán fordított előjelű (de nem veszélyes) változás, hogy számos olyan funkció vagy beállítás került be a standard felhasználók jogosultsági körébe, amelyekre korábban nem volt lehetőség, (ezt később bővebben is kifejtjük), de azért még mindig maradt rengeteg, amelyhez ennél több jogosultság szükséges.

Ha olyan műveletre kerül sor, amikor valóban hozzá kell nyúlni bizonyos rendszerbeállításokhoz, vagy olyan védett mappákba kell programot telepíteni, mint a *\Windows* vagy a *\Program Files*, a Vista interaktivitásra készteti a felhasználót, azaz egy úgynevezett „eleváló" promptot, jogosultság-jóváhagyó kérdést küld a felhasználónak. Azaz a standard felhasználónak külön engedélyeznie kell, mikor a rendszergazda jogaival élni szeretne. Ez lehetőséget biztosít a felhasználónak, hogy eldöntse, egy alkalmazás élhet-e ezekkel a jogokkal. Ez egyben azt is jelenti, hogy a felhasználó minden esetben információt kap arról, milyen alkalmazások indulnak el, amelyek rendszergazdai joggal futnak.

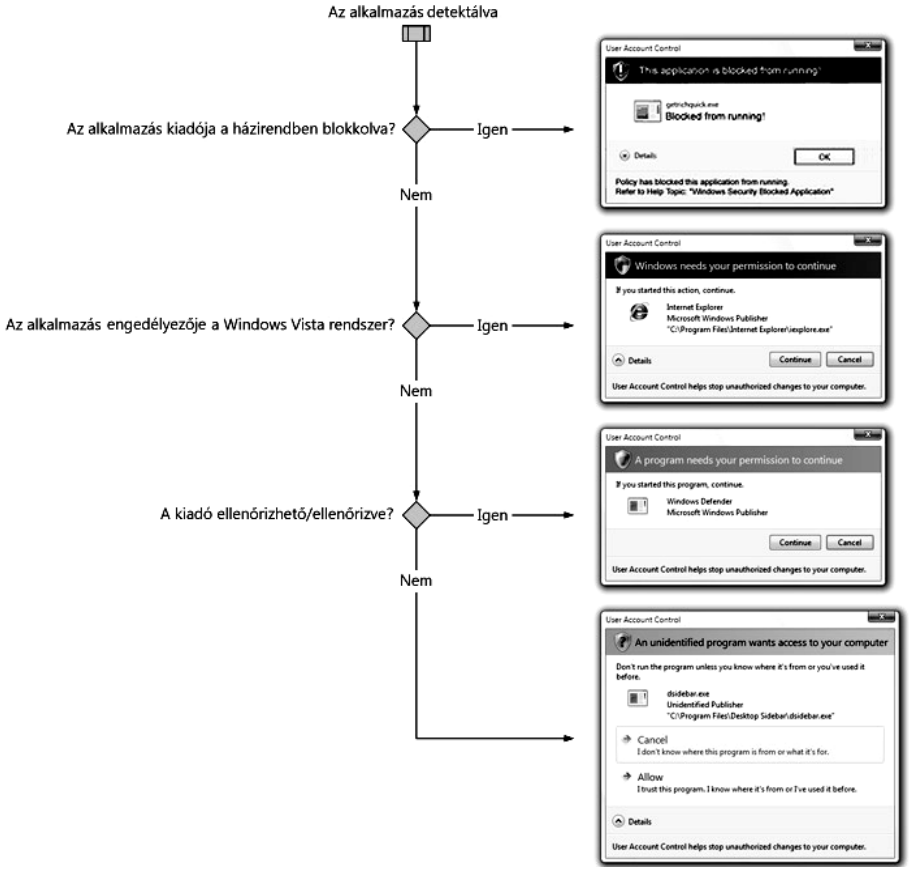
A technikai magyarázat lényege, hogy amikor egy felhasználó bejelentkezik, az UAC két biztonsági tokent hoz létre. Egy „normál" felhasználói tokent és egy olyan tokent, amely tartalmazza a rendszergazda jogokat. Az elindított folyamat akkor nem kapja meg az utóbbi jogokat, ha a felhasználó a folyamat indulásakor nem engedélyezi az UAC felületén keresztül. A létrejött „normál" felhasználói tokenben az alábbi különbségeket fedezhetjük fel – szemben a rendszergazdai tokennel (az ismeretlen fogalmakra később visszatérünk):

- Kilenc rendszergazda-szintű jog nincs benne.
- A felhasználó integritási szintje *Medium*, és nem *High*.
- Alkalmazódik rá egy alapesetben mindent tiltó SID.
- Megjelenhet számára az UAC engedélyező ablak *(consent.exe)*.
- Fájl- és regisztrációs adatbázis virtualizáció alkalmazódhat rá.

Az UAC különféle helyzeteknek megfelelően többfajta engedélyező ablakot jeleníthet meg. Ha az alkalmazás, vagy annak kiadója a biztonsági házirend szerint blokkolva van, egy piros fejléccel rendelkező figyelmeztető ablak jelenik meg, a program futtatása pedig nem lehetséges. Kékes-zöldes színű ablakot láthatunk, ha a jogosultsági szint emelését a Windows egyik beépített komponense kéri. Külső programok esetén szürke színkódú UAC-promptot kapunk, ha az állomány rendelkezik digitális aláírással, így az valószínűleg megbízható forrásból származik, figyelemfelkeltőbb, sárga színűt pedig, ha nem található aláírás – ez esetben csak akkor futtassuk az alkalmazást, ha ismerjük származási helyét és teljesen megbízunk abban.

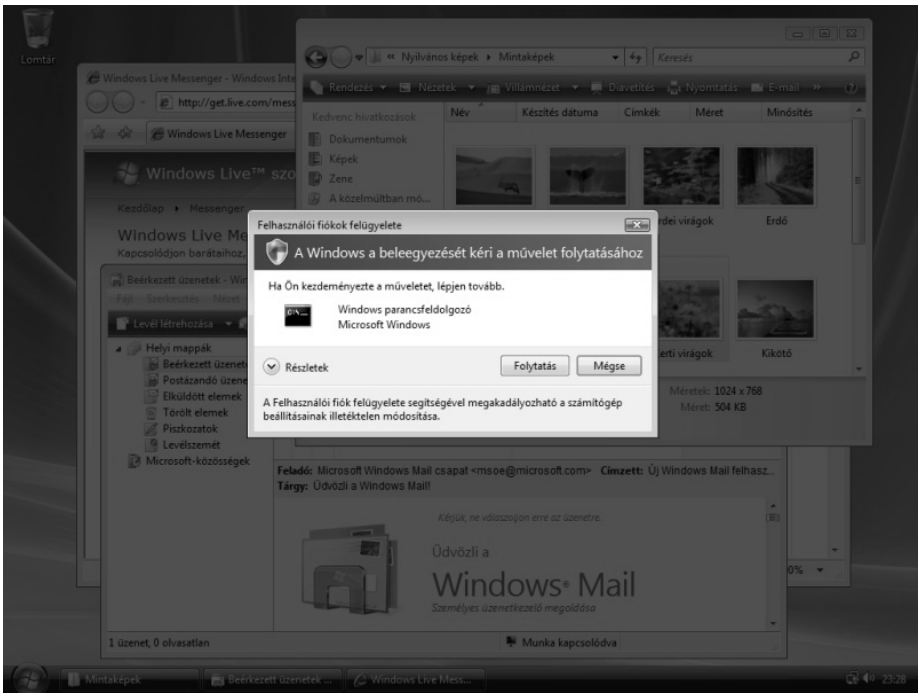
A User Account Control részletes beállítása a helyi biztonsági házirendből történhet. A finombeállítások között megadhatjuk például, hogy a figyelmeztető kérdés rendszergazda-jogosultságú felhasználó esetén csak egy igen/nem választási lehetőségből, vagy akár teljesen egy figyelmezetés nélkül történjen, vagy például azt is, hogy egy standard felhasználó esetén egyáltalán ne legyen lehetőség a név/jelszó páros megadására, hanem csak az elutasításra.

Történetesen még azt is beállíthatjuk, hogy az UAC a kérdőablak megjelenítésekor átkapcsoljon-e az úgynevezett *Secure Desktop* módba. A házirendből (és a *Control Panel / User Accounts* pont alól) akár ki is kapcsolhatjuk az UAC-t, de ez természetesen nem ajánlott.



3.18. ábra: *A különböző UAC-párbeszédablakok a kód ellenőrzésének folyamata szerint*

A Secure Desktop a felhasználó munkafolyamatában, de elszeparált asztalként jön létre, ráadásul csak a rendszer által írható, így a biztonsági asztalt semmilyen külső, a felhasználó asztalán futó folyamattal nem lehet befolyásolni. Ez szinte tökéletesen megbízhatóvá teszi a Secure Desktopon megjelenített ablakokat, vagyis biztosak lehetünk benne, hogy maga a rendszer és nem pedig egy vírus küldte a megtévesztő üzenetet.



3.19. ábra: *A Secure Desktop állapot*

Az alábbiakban azon események (nem teljes) listáját láthatjuk, amikor az UAC szolgáltatás közbelép:

- Alkalmazások telepítése és eltávolítása.
- Eszközmeghajtó programok telepítése és eltávolítása.
- ActiveX-vezérlők telepítése.
- Windows-frissítések telepítése.
- A Windows Update beállításainak módosítása.
- A Windows tűzfal beállításainak módosítása.
- A Felhasználói fiókok felügyelete (UAC) beállításainak módosítása.
- Felhasználói fiókok létrehozása és törlése.
- Felhasználói fiókok típusának megváltoztatása.
- A szülői felügyelet konfigurálása.
- A feladatütemező megnyitása.

- Rendszerfájlok biztonsági mentésből történő visszaállítása.
- Más felhasználó mappájának megnyitása vagy megváltoztatása.

A korlátozott jogkörben dolgozó felhasználók alapértelmezésként az UAC felügyelete alatt dolgoznak, mely esetükben a fenti felsorolásban szereplő műveleteknél nem egy egyszerű engedélyező ablakot jelenít meg, hanem egy rendszergazda jogosultságú felhasználó hitelesítő adatait kéri be (de – ahogyan korábban említettük – ez a működés a biztonsági házirendből megváltoztatható). Anélkül, hogy az UAC-cal találkoznának, a standard jogú felhasználók az alábbi műveleteket végezhetik el (szintén nem teljes a lista):

- Vezeték nélküli hálózat konfigurálása.
- Energiaellátási opciók változtatása.
- VPN-kapcsolatok konfigurálása.
- Nyomtató és egyéb eszközök hozzáadása (házirendből szabályozva).
- Windows Update használata.
- Windows Defender használata.
- Lemezdefragmentálás, Disk Cleanup futtatása.
- Időzónaváltás.
- Eseménynapló megtekintése (kivéve persze a Security naplót).

Ha egy program futása közben szükségtelenül generál szintemelést kérő párbeszédablakot, a Microsoft alkalmazáshibaként tekint az esetre, tehát (ha pl. az *Error Reporting*-szolgáltatás révén beérkezik), úgy kezeli a helyzetet, mintha a program hibásan működne. Ezzel magas prioritást kapnak az efféle problémák, tehát a fejlesztők is hamarabb reagálhatnak rá, ezért egyre biztosabbak lehetünk abban, hogy valóban csak akkor jelenik meg az UAC-prompt, amikor tényleg szükség van rá – feleslegesen nem bukkan fel.

A Vista további praktikus megoldásokkal is segíti az UAC-prompt esetlegesen indokolatlanul zavaró és állandó megjelenését:

- Lehetővé teszi a rendszergazdáknak, hogy meghatározzák, a nem rendszergazda-jogú felhasználók milyen meghajtóprogramokat, eszközöket, ActiveX-vezérlőket telepíthetnek. Így, adott esetben, a nem rendszergazdai jogú felhasználók is telepíthetnek nyomtatókat, VPN-szoftvereket stb.

- Alap hálózati konfigurációk elvégzéséhez a felhasználót elegendő hozzáadni a Network Configurations Operators csoporthoz. Ennek a csoportnak joga van az IP-címek megváltoztatásához, DNS-cache ürítéséhez stb., vagyis a nélkül végezhetők el ezek a feladatok, hogy a felhasználó az Administrators *(Rendszergazda)* csoporttagságra lenne szükségük.
- Az UAC-fájlrendszer és regisztrációs adatbázis virtualizációja és a beépített alkalmazás kompatibilitási sémák segítségével sok rendszergazdai jogokat igénylő alkalmazás futtatását teszi lehetővé, számos problémán segít (a részleteket lásd a következő alfejezetben).

Az UAC tervezésekor felállított programozási irányelvek kimondják, hogy a felhasználónak mindig előre tudnia kell róla, ha a művelet jogosultsági szintemelést követel. Ezt a gombokon és hivatkozások mellett elhelyezett kis pajzsok ( ) jelzik, egyértelművé téve, mely műveletekhez szükséges emelt szintű hozzáférés.

A fiókváltozások és a User Account Control (UAC)
Ebben az előadásban a Vista felhasználói fiókjaival és csoportjaival, illetve a talán legfontosabb a biztonságot érintő változással, az UAC-lal kapcsolatos részleteket tárjuk fel.
Fájlnév: I-3-3b-Fiokok-es-UAC.avi

Fájl- és registryvirtualizáció

A User Account Control egy másik fontos feladata a szoftverkörnyezet virtualizálása azon alkalmazások számára, melyek nem lettek felkészítve a többfelhasználós rendszerekre, vagy nem kezelik jól a jogosultságokat. Egyelőre meglehetősen sok olyan program létezik, amely vagy nem veszi figyelembe, hogy többfelhasználós környezetben működik, vagy egyszerűen nem is hajlandó futni, csak és kizárólag rendszergazdai jogosultságokkal. Az UAC ezért detektálja az alkalmazás fájlrendszerbe és a registrybe való írási kéréseit, és ennek megfelelően – minden felhasználói fiókban egyéni – virtuális környezetet (úgynevezett „homokozót") hoz létre a programnak.

A rendszergazda-jogosultságot megkövetelő programok így tulajdonképpen „azt hiszik", hogy tudnak írni a pl. a *\Windows*, vagy a *\Program Files* mappákba, esetleg a rendszerleíró adatbázis kritikus részeibe is, ám valójában egy, a számukra létrehozott virtuális valóságban működnek – immáron gond nélkül. A virtualizált mappákat a védett rendszerkönyvtárak tallózásakor megjelenő *Compatibility Files* gombra kattintva nyithatjuk meg, ezek fizikai helye a felhasználó profilkönyvtárában található az alábbi útvonalon: *\Users\<felhasználónév>\AppData\Local\VirtualStore*.

A regisztrációs adatbázist érintő írási műveletek pedig a *HKCU\Software\Classes\VirtualStore* kulcs alá kerülnek.

Mint az útvonalakból is látható, mind a két hely a felhasználó profilja alatt helyezkedik el, így a felhasználónak van rá írási joga. Ha felhasználónkénti szabály nem definiálja másképp, az olvasás elsőként a globális helyről történik. A fájlrendszer virtualizációja egy filter driver *(luafv.sys)* segítségével valósul meg, a regisztrációs adatbázisé pedig beépítetten.

A fájl- és regisztrációs adatbázis virtualizáció meggátolja az írásokat a nem adminisztrátori jogú (nem elevált) folyamatok számára, de csak az alábbi helyekre:

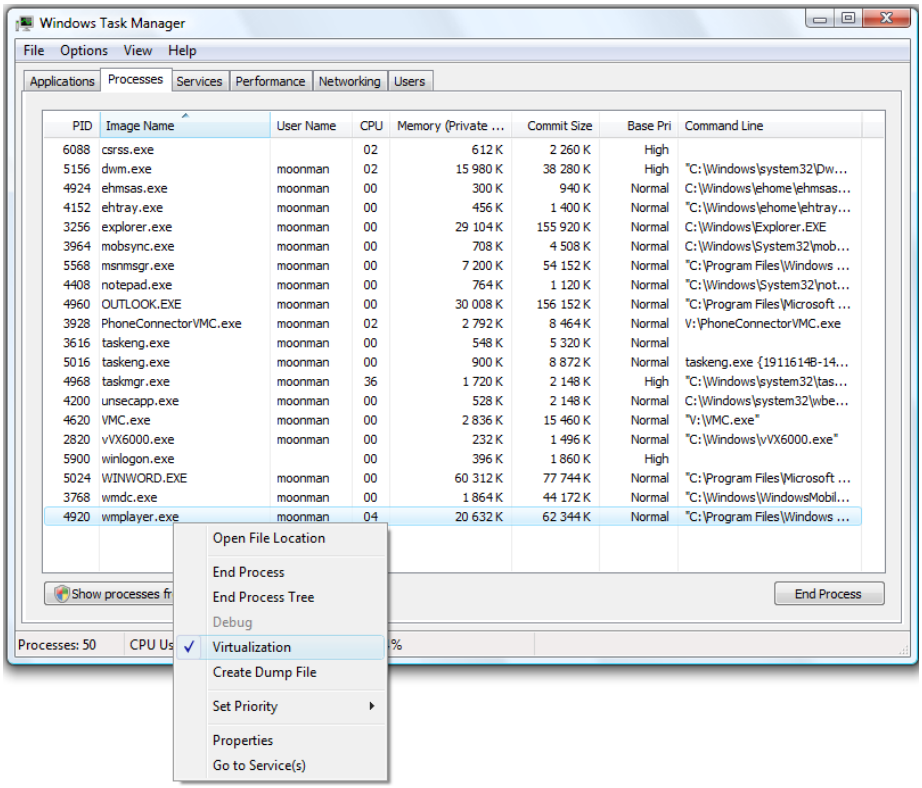
- *\Program Files* és az almappái.
- *\Program Files* (x86) 64-bites rendszereken.
- *\Windows* és almappái, beleértve a System32-t is.
- *\Users\%AllUsersProfile% \ProgramData*
- *HKLM\Software*

Az alábbi objektumok azonban soha sem kerülnek virtualizálásra:

- Vista alkalmazások.
- Futtatható állományok, mint az *.EXE, .BAT, .VBS* és *.SCR*. A további fájlrendszeri kivételek a *HKLM\System\CurrentControlSet\Services\Luafv\Parameters\ExcludedExtensionsAdd* kulcsban adhatóak meg.
- 64-bites alkalmazások és folyamatok.
- Azok az alkalmazások, amelyeknél gyárilag definiálva van, hogy nem virtualizáltan futtatandók (mint az összes Vista-komponens).
- Folyamatok és alkalmazások, amelyek rendszergazdai jogokkal futnak.
- Kernelmódú alkalmazások.
- Műveletek, amelyek nem interaktív bejelentkezésből származnak (pl.: fájlmegosztáson keresztüli elérés).
- Alkalmazások amelyek a regisztrációs adatbázisban a *Dont_Virtualize* jelzéssel vannak megjelölve.

Az utolsó ponthoz tartozó plusz információ: a *reg.exe* segítségével láthatjuk a három új *registry flag*-et a *HKLM\Software* kulcs alatt, ezek a következőek: *DONT_VIRTUALIZE, DONT_SILENT_FAIL, RECURSE_FLAG*

Az egyes alkalmazások virtualizációját a Task Managerből *(Feladatkezelő)* akár saját magunk is engedélyezhetjük (vagy tilthatjuk le). Ezt a műveletet ajánlott csak szükség esetén elvégezni, kiváltképp a Windows beépített folyamatainál, mert a téves konfiguráció akár a rendszer instabil működéséhez is vezethet.



3.20. ábra: *A feladatkezelőben a „közönséges" processzeket egyszerűen virtualizálhatjuk*

Fájl- és registryvirtualizáció
Ebben a screencastban több példát is hozunk az UAC „melléktermékeként" megjelent fájl- és registryvirtualizációra, először egy dedikált alkalmazás majd a cmd.exe segítségével.
Fájlnév: I-3-3c-Fajl-es-registry-virtualizacio.avi

Mandatory Integrity Control (MIC)

A következőkben bemutatott kerülő védelmi eljárás még egy, az 1970-es években született elgondoláson alapszik, megvalósítására azonban csak napjainkban került sor. Míg a fájlrendszer-jogosultságok könnyen kezelhető és hatékony védelmet nyújtanak az illetéktelen hozzáférésektől, a technológia rendelkezik némi korlátoltsággal. Hiába védjük másoktól a fájlokat, ha magát a tulajdonost is viszonylag könnyen rávehetjük, hogy lefuttasson egy-egy parancsot – természetesen adminisztrátori jogokkal. A MIC alapelgondolása a következő: a csökkentett megbízhatósági szinten dolgozó alanyok nem módosíthatnak magasabb szinten lévő objektumokat, a magasabb szinten létező objektumok pedig nem kényszeríthetők, hogy megbízzanak alacsonyabb szintről érkező utasításokban vagy adatokban. A kulcsszó itt a „megbízhatóság", a MIC pedig ezt az információáramlási szabályt valósítja meg a Windows Vistában.

Amikor bejelentkezünk, a Windows egy adott integritási azonosítót rendel a felhasználónkhoz. Ez az azonosító tartalmazza mindazt az információt, amiből a rendszer megállapítja, hogy mely területekhez van hozzáférésünk, és melyekhez nincs. Nem csak a felhasználók, de a védeni kívánt rendszerobjektumok, úgy mint fájlok, mappák, adatcsatornák, folyamatok (processzek), folyamatszálak (threadek), az ablakkezelő, registrykulcsok, szolgáltatások, nyomtatók, megosztások, ütemezett feladatok stb. is kapnak egy-egy saját szintazonosítót. Ezek az azonosítók a System Access Control Listben (SACL) tárolódnak.

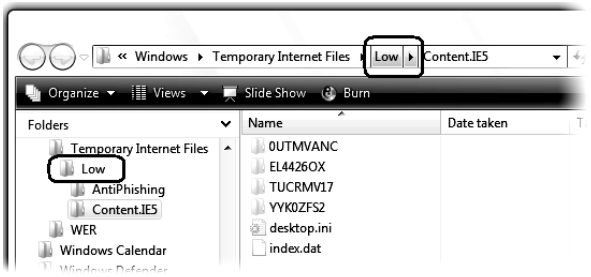
Amikor a felhasználó egy műveletet végez, a Windows még azelőtt, hogy a fájlrendszer-jogosultságokat vizsgálná, összehasonlítja a felhasználó integritásszintjét a műveletben részt vevő objektumokéval. Ha a felhasználó szintje a domináns – vagyis az objektuméval megegyező vagy magasabb – a Windows engedélyezi a feladat végrehajtását – feltéve, hogy fájlrendszerszinten is megvan hozzá a kellő engedélye. Ha a felhasználó alacsonyabb szintről próbál manipulálni egy objektumot, a Windows nem engedélyezi a hozzáférést, függetlenül attól, hogy magához a fájlhoz, registrykulcshoz, vagy egyéb komponenshez különben meglenne a hozzáférése. Láthatjuk tehát, hogy az integritásszintek minden esetben a fájlrendszer-jogosultságok, vagyis az ACL fölött állnak.

A Windows Vistában négy integritásszintet definiáltak a fejlesztők: Low *(alacsony)*, Medium *(közepes),* High *(magas)* és a System *(rendszer).* Az egyszerű felhasználók közepes, a (valódi) rendszergazda jogosultságúak pedig magas szinten tevékenykednek. A felhasználó által indított folyamatok vagy az általa létrehozott objektumok öröklik a felhasználó integritásszintjét, a rendszerszolgáltatások a „rendszer" szintre kapnak belépőt. Ha valamilyen okból kifolyólag egy objektum nem kap integritásszint-jelölést, az operációs rendszer automatikusan közepes szintre sorolja be, ezzel megakadályozva, hogy az alacsony szinten futó folyamatok hozzáférhessenek a nem jelölt ob-

jektumokhoz. Az operációs rendszer fájljai alapértelmezésként nem jelöltek, így közepes szinten tartózkodnak, valamint természetesen alkalmazódnak rájuk a megfelelő fájlrendszer-jogosultsági beállítások (ACL) is. Az egyes objektumok integritási szintjei a SACL-ekben tárolódnak és az ellenőrzésük minden esetben a DACL ellenőrzések előtt történik.

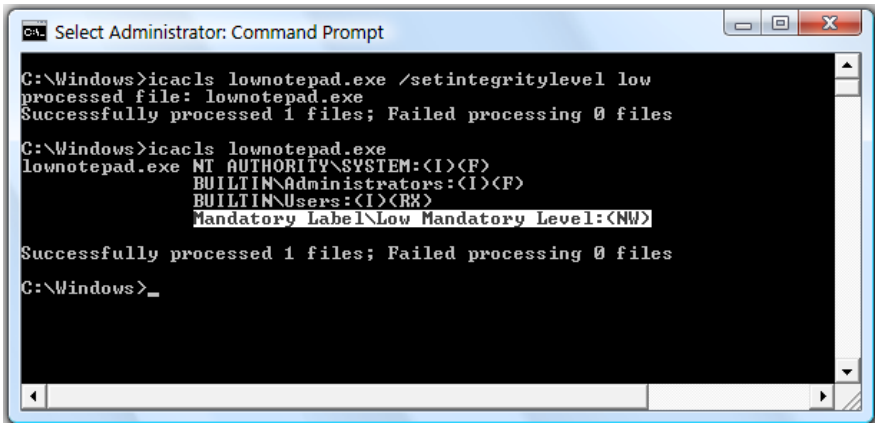
Szint	SID	Hex érték	Használati példák
Low	S-1-16-4096	1000	Védett módú Internet Explorer
Medium	S-1-16-8192	2000	Hitelesített felhasználók/ Nem elevált
High	S-1-16-12288	3000	Rendszergazdák/ Elevált jogok
System	S-1-16-16384	4000	Helyi rendszer

Hogy miért szükséges ez a bűvészkedés a jogosultsági szintekkel? Képzeljük el a következő helyzetet: kapunk egy e-mailt egy csatolt fájllal. Amikor lementjük a fájlt, az rögtön alacsony integritásszintre kerül, mivel az internetről (azaz egy nem megbízható helyről) érkezett. Ezért aztán bármi legyen is a fájl tartalma, amikor lefuttatjuk, semmi különös nem történhet, mivel a fentiek alapján egy alacsony szinten futó folyamat nem férhet hozzá a felhasználó magas, vagy nem jelölt, így közepes szinten lévő adataihoz.



Az Internet Explorer védett módja a megbízhatósági szintek köré épült, és – mivel a böngésző alapértelmezésként alacsony *(Low IL)* integritásszinten fut – biztosak lehetünk benne, hogy az Internet Exploreren keresztül hozzájárulásunk nélkül nem települhet többé a rendszerre semmilyen ártó kód. Ezen túlmenően, mivel a Windows munkaasztal közepes szintre van besorolva, a böngészőben esetlegesen lefutó ActiveX-vezérlő sem küldhet többé olyan megtévesztő üzeneteket az asztalra, miszerint vírustámadás áldozatai lettünk, és azonnali hatállyal töltsünk le egy bizonyos programot – ami valójában maga a vírus.

Az NTFS fájlrendszer-jogosultságokhoz hasonlóan – bizonyos korlátok között – az integritásszinteket is az *icacls* paranccsal kezelhetjük. Két korlátozás létezik: az objektumokat nem helyezhetjük át a System, illetve az Untrusted szintekre. Az integritásszintek változtatásához használjuk a */setintegritylevel* kapcsolót, azonban bánjunk óvatosan ezzel az eszközzel és csak szükség esetén módosítsuk ezt az objektumtulajdonságot!



3.21. ábra: *Sikeres integritási szint beállítás parancssorból*

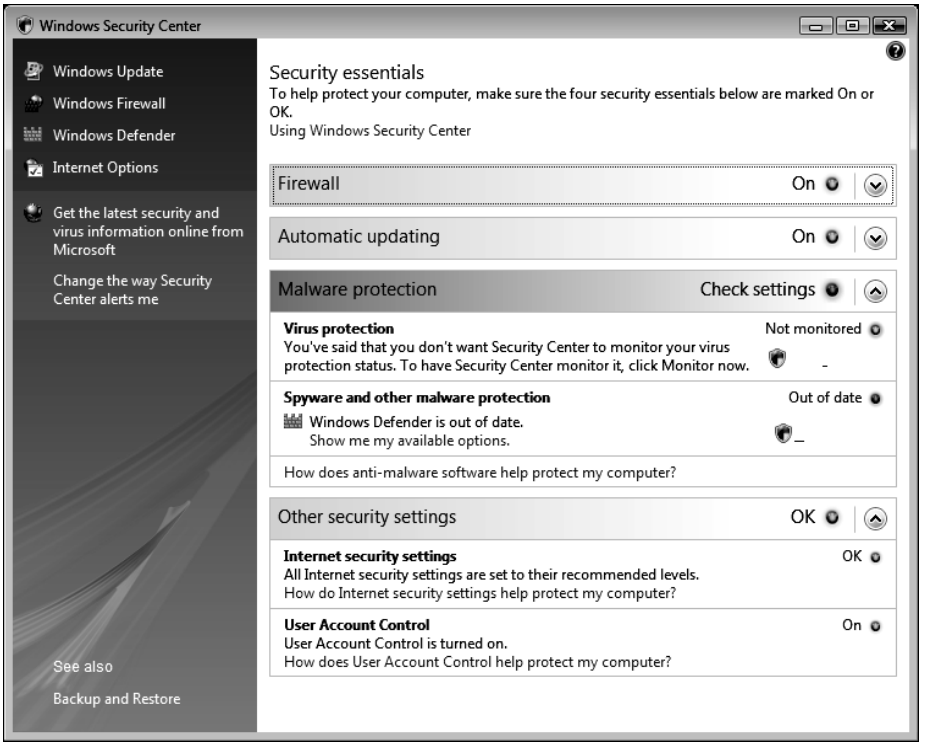
A biztonsági rendszer összetevői

A következő alfejezetben a Vista olyan a biztonságához kapcsolódó komponenseinek lehetőségeit és alkalmazási területeit foglaljuk össze, amelyekkel már sűrűbben találkozunk a felszínen is. Természetesen itt elsősorban az üzemeltetők jelentik a hatókört, akiknek akár a napi feladatai közé is tartozhat a Security Center jelzéseinek értelmezése, az Internet Explorer 7-es változatának precíz beállítása és új lehetőségeinek ismerete. De a Windows Defender, az EFS, a BitLocker vagy akár a Vista új tűzfalának mélyreható megismerését sem érdemes kihagyni – főképp, ha a feladataink közé tartozik az ügyfélszámítógépek biztonságos működtetése.

A Security Center

A Windows Vistába beépített Security Center *(Biztonsági központ)* sokban hasonlít a korábbi verzióhoz, azonban el is tér attól. A tűzfal, az Automatikus frissítések ügyfél és a vírusirtó állapotának állandó vizsgálata megmaradt, viszont bekerült a monitorozandó komponensek közé az immár integrált Windows Defender (lásd később) a frissítési opcióval együtt.

Az UAC működése szintén nyomon követhető a Security Centerben, valamint egy teljesen új szakasszal is bővültek a lehetőségeink, azaz az Internet Explorer legfontosabb biztonsági beállításait is ellenőrzi a rendszer, és jelzést is kapunk, ha ezek állapotában negatív változás következik be (a megfigyelt paraméterekről további részleteket olvashatunk kicsit később, a „Biztonsági beállítások automatikus felügyelete" szakaszban).



3.22. ábra: *A Windows Vista Security Center tartalma bővült*

A Windows XP és a Windows Vista Biztonsági központja *(Security Center)*
Ennek az előadásnak a témája a két operációs rendszer Biztonsági központjának bemutatása.
Fájlnév: I-3-4a-Security-Centers.avi

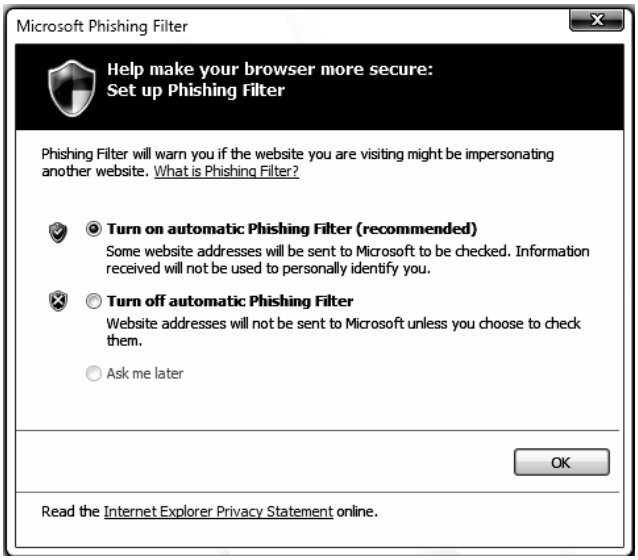
Az Internet Explorer 7 biztonsági újításai

A korábbi ügyfél operációs rendszerekben, és különösen a Windows XP Service Pack 2-ben már jelentős változások voltak tapasztalhatóak a Microsoft böngészőprogramjával kapcsolatban – elsősorban a biztonságosságot tekintve. Lehetővé vált pl. a felugró ablakok blokkolása, valamint módosult (lényegesen szigorúbb lett) az ActiveX vezérlők kezelése is, és megjelent a figyelemfelkeltő biztonsági sáv is.

A Windows Vistába már a böngésző következő, 7.0-s verziója került, mely jó pár régóta várt funkciót hozott. Először is lehetővé vált a füles/lapos navigálás, valamint egyéb olyan biztonsági megoldások is beépültek, mint például az opt-in (engedélyezendő) ActiveX-kezelés, a továbbfejlesztett bővítménykezelő, az adathalászat *(phishing)* elleni védelem, valamint a védett módú böngészés *(Protected Mode)*. A tanúsítványkezelés és a haladó beállítások területén is tapasztalhatunk pozitív változásokat.

Ugyan a Windows XP-re és a Windows Server 2003-ra is letölthető az Internet Explorer 7-es változata, de ezek mégsem egyeznek meg mindenben a Vistába integrált változattal. A különbségek az eltérő biztonsági háttérből adódnak: a Vistánál használt IE7 olyan lehetőségeket is képes alkalmazni, amelyek az UAC jelenlétének a következményei, pl. az ún. védett mód (lásd később).

Phishing filter



3.23. ábra: *Az IE7 első indításakor rögtön bekapcsolhatjuk az adathalászat-szűrőt*

Napjaink egyik legelterjedtebb online bűnözési formája, az úgynevezett adathalászat, a phishing. Ennek az a lényege, hogy például olyan pénzügyi szolgáltatásnak álcázott webhelyre csalják a felhasználót, mely külsőre szinte pontosan megegyezik egy-egy bank vagy pénzintézet honlapjával. Itt aztán a felhasználótól olyan személyes adatokat kérnek be, melyek felhasználásával hozzáférhetnek bankszámlájához és egyéb személyes értékeihez. A phishing elleni védelem központi szerepet kapott az Internet Explorer 7-ben, a böngésző első indításakor máris lehetőségünk van a szűrő bekapcsolására és a beállítások testreszabására. Az IE7 phishing filtere rendszeresen frissülő online adatbázison és egy intelligens szűrőn alapul, mely tipikus jellemzők után kutatva megvizsgálja a weblap eredetiségét és megbízhatóságát. Ha e vizsgálat során nem találja megfelelőnek az adott oldalt, akkor ezt szembetűnően jelzi a felhasználónak.

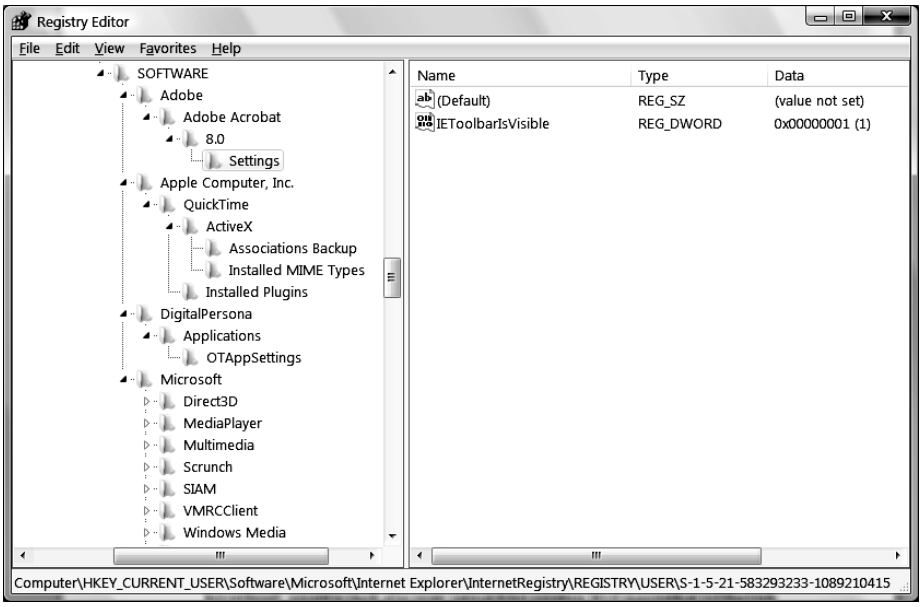
Védett mód

Az előző részben ismertetett User Account Control nemcsak a figyelmeztető ablakok küldésével próbálja kordában tartani a felhasználókat, de neki köszönhetjük, hogy az Internet Explorer 7 képes úgynevezett védett módban *(Protected mode)* futni – de csak a Vistán, az XP-re telepített IE7 nem ismeri ezt a fajta működést.

Ha a védett mód engedélyezve van, az IE7 nagyon alacsony integritási szinten *(Low IL)* dolgozik, amely számos biztonsági korlátot jelent a működésben. Ezek közül az egyik az, hogy a rendszer biztonsági alapbeállításainak megváltoztatása vagy egy emelt szintű jogosultság nélkül egy website nem képes semmilyen módon egy alkalmazást telepíteni a böngészőn keresztül. Ez azért van, mert az alacsony integritási szintnek köszönhetően a böngésző a fájlrendszerbe, illetve a registrybe nem írhat automatikusan. Mivel a különböző integritási szinten lévő processzek közötti kommunikáció szintén erősen limitálva van, a kényszerűen hasonlóan alacsony szinten működő ActiveX-vezérlők és az extra eszköztárak sem képesek hozzáférni semmilyen fontos rendszerelemhez.

Ezen kívül a Vista egy speciális virtuális mappát is előkészít az IE7 számára, az olyan fájlok tárolásához, amelyeket a böngésző menetközben egyébként a számára tiltott helyekre mentene el. Ez a mappa szokásos gyorsítótáron belül helyezkedik el *(Temporary Internet Files\Low)*, és ide és csak ide képes egy alacsony integritási szinttel rendelkező folyamat írni. Gyakorlatilag ez a korábban ismertetett fájl- és registryvirtualizáció elve alapján működik, csendben a háttérben, sikeresen megtévesztve bővítményeket, vagy a bármit, amely az IE7 alatt tevékenykedik.

A teljesség kedvéért említsük meg, hogy a rendszerleíró adatbázist érintő írási próbálkozások ugyanezzel a módszerrel, ugyanígy végzik, egy – szintén – elkülönített területen *(HKCU\Software\Microsoft\Internet Explorer\InternetRegistry\REGISTRY\USER\{a_user_SIDje}\Software)*.



3.24. ábra: *A bővítmények „homokozója" a registry elkülönített részében*

De mi történik, ha az IE7 mégis ki akarja „olvasni" ezt az elkülönített, virtualizált tartalmat, azaz pl. egy rendszergazda szeretne egy ActiveX-vezérlőt telepíteni? Egy ún. broker processz beavatkozik, azaz megerősítést kér a folytatás előtt, és jön az ismerős UAC-prompt és a felhasználói interaktivitás.

A színfalak mögött a Vista további mappákat is létrehoz a védett módú működés kiszolgálása céljából, azaz a böngésző rendszeres használatával a következő, szintén csak alacsony integritási szinten lévő mappákat tölthetjük meg fájlokkal, a szokásos böngésző mappák helyett:

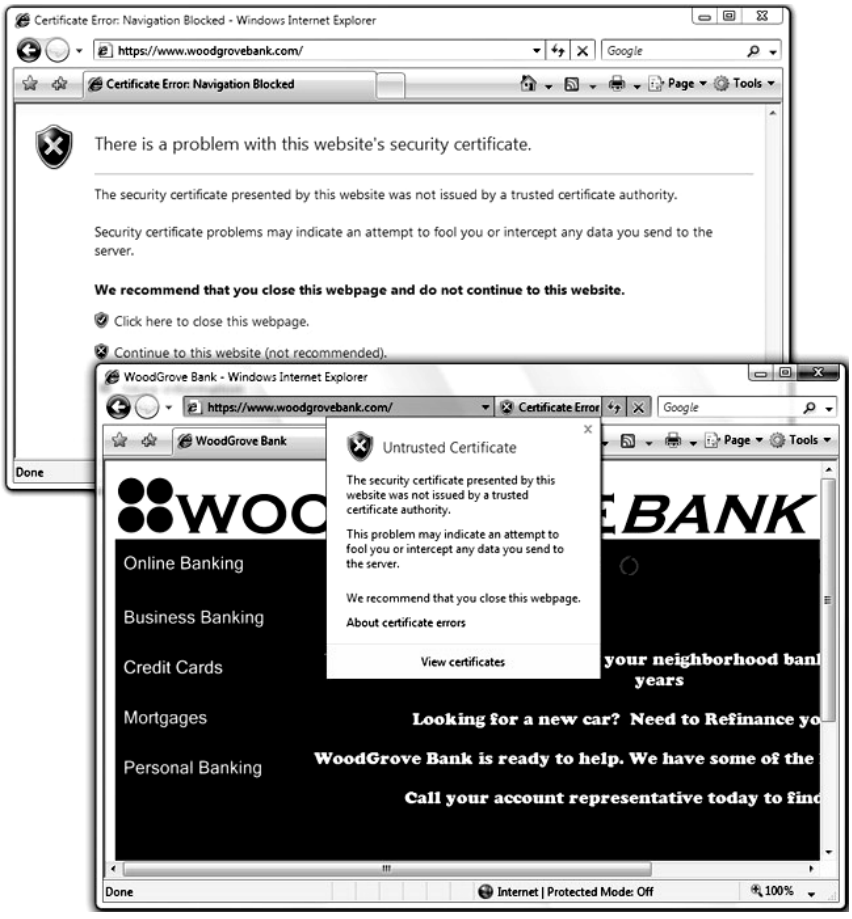
- **Temp**: %LocalAppData%\Temp\Low
- **Cookies**: %AppData%\Microsoft\Windows\Cookies\Low
- **History:** %LocalAppData%\Microsoft\Windows\History\Low

A védett mód alapértelmezés szerint be van kapcsolva az Internet, Helyi intranet *(Local intranet)* és Tiltott helyek *(Restricted sites)* zónákban (a Megbízható helyek *(Trusted sites)* zónában tehát nem), a bekapcsolt állapotot pedig egy, az állapotsorban látható ikon jelzi.

A védett mód alapértelmezésként aktív, kikapcsolása – hacsak nem abszolút megbízható helyen, például céges intraneten böngészünk – nem ajánlott, már csak azért sem, mert ekkor az IE automatikusan a közepes integritási szintre „kapaszkodik fel".

Tanúsítvány-ellenőrzés

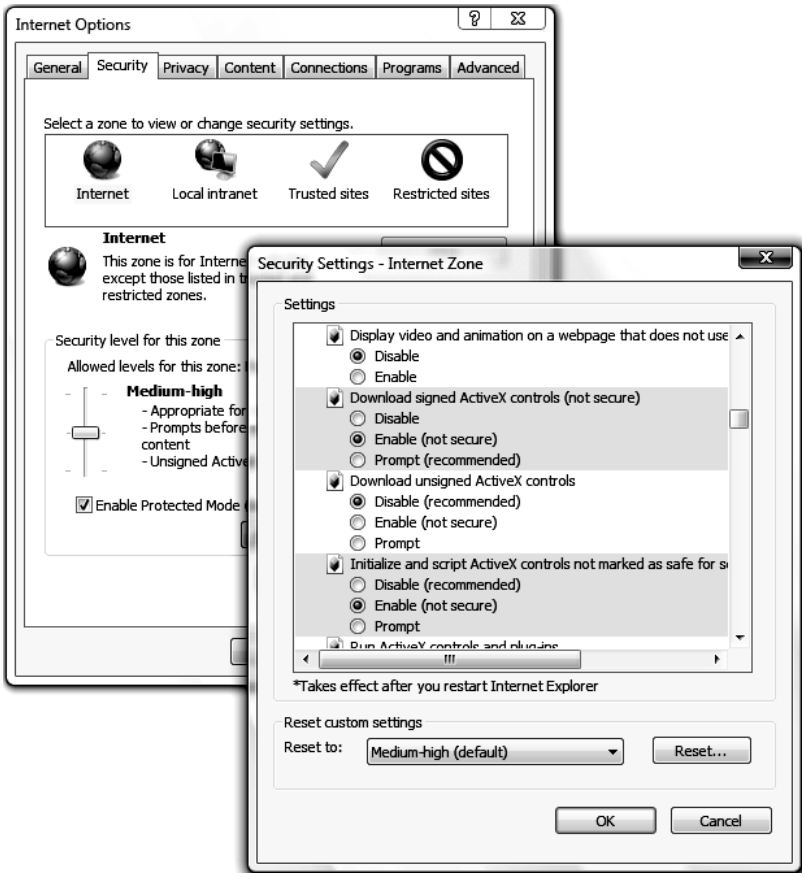
Az érvénytelen tanúsítvánnyal rendelkező oldalak meglátogatásakor eddig is kaptunk figyelmeztetést, most azonban olyan hangsúlyos lett a biztonsági riasztás, hogy az a kezdő felhasználók figyelmét sem kerülheti el. A megbízható, erős titkosítást használó oldalak címe mellett egy lakat ikon jelzi a biztonságos kapcsolatot, a veszélyesnek minősített oldalak címsora pedig pirosra változik. Az érvénytelen, vagy lejárt érvényességi idővel rendelkező tanúsítványt használó weblapok továbbra is megtekinthetők, előtte azonban a felhasználónak nyugtáznia kell, hogy megértette a kockázati tényezőket és saját felelősségére lép be az oldalra.



3.25. ábra: *A figyelmeztetés nyilvánvaló: ez a tanúsítvány nem megfelelő*

Biztonsági beállítások automatikus felügyelete

Az Internet Explorer 7 képes detektálni, ha az adott zónának megfelelő biztonsági beállítások eltérnek az alapértelmezett szinttől és veszélyesek lehetnek a böngészésre nézve. A biztonsági sávra kattintva lehetőségünk van a problémás beállítások automatikus korrigálását kérni, vagy a konfigurációs panelt megnyitva kézzel módosítani azokat.



3.26. ábra: *A zóna biztonsági opciók között kiemelve látjuk az igazán fontosakat*

Ha a manuális módszer mellett döntünk, segítségünkre lehet, hogy az Internet Explorer piros színnel megjelöli számunkra a veszélyesnek ítélt beállításokat. A zónabeállítások között olyan újdonságokat találunk, mint a felbukkanó szkriptelt ablakok tiltása, a státuszsor weboldal általi frissítésének letiltása, valamint immár minden egyes ablaknak kötelező jelleggel látszik a cím- (URL) és állapotsora. Ezekre a korlátozásokra szintén az egyre terjedő adathalász-támadások kivédése miatt van szükség.

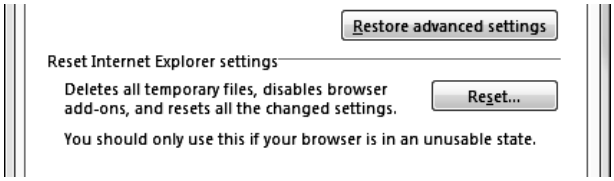
Haladó lehetőségek és beállítások — egyszerű problémamegoldás

Ha tallózzuk a Start menüt, az *Accessories \ System Tools (Kellékek/Rendszereszközök)* programcsoportban rátalálhatunk egy speciális IE-változatra, amelyet Internet Explorer (No Add-ons) névvel láttak el. Ezzel az ikonnal egy teljesen csupasz, bővítmények és extra eszköztárak nélküli böngészőt indíthatunk el, azaz az esetleg, már jó alaposan beépült rosszindulatú vagy hibás működésű bővítmények használata kikerülhető. Ezt a problémamegoldáshoz nagyon hasznos üzemmódot egyébként elérhetjük a parancssorból is, a következő paranccsal: *iexplore -extoff*.

A biztonság fokozója az a speciális, az Internet Options\General *(Internet-beállítások/Általános)* fülről elérhető panel is, amelyben egy menetben törölhetjük az IE gyorsítótárát, a komplett előzménylistát, a sütiket, a különböző űrlapokba beírt és eltárolt adatokat, valamint az internetezés során itt-ott megadott jelszavakat.

3.27. ábra: *Érzékeny adatok egyszerű törlése*

Végül, de nem utolsósorban említsünk meg még két szintén haladó opciót, amelyek az Internet Options\ Advanced *(Internetbeállítások/Speciális)* fülön találhatóak, a panel alján a kiemelt opciók között Az egyikkel (Restore advanced settings – *Speciális beállítások visszaállítása)* könnyedén visszaállítható az összes haladó beállítás, amely szép számban, ugyanezen a panelen találhatóak. A másikkal viszont az egész Internet Explorert totális alaphelyzetbe hozhatjuk (Reset Internet Explorer Settings – *Alaphelyzet),* amely bizonyos esetekben igencsak hasznos és gyors megoldásnak bizonyulhat.



3.28. ábra: *Az IE7 biztonsági opcióinak alaphelyzetbe állítása egyszerű*

Az Internet Explorer 7.0 biztonsággal kapcsolatos újdonságai
Ebben az előadásban online példákkal mutatjuk be az itt felsorolt újdonságokat és változásokat az Internet Explorer 7-tel kapcsolatban.
Fájlnév: I-3-4b-IE7-biztonsag.avi

A Windows Defender

A Microsoft eredetileg a Windows XP-hez kezdte fejleszteni „Microsoft Anti-Spyware" néven kémprogram és trójai-figyelő alkalmazását, melynek végleges verziója a Windows Defender nevet kapta, és végül a Windows Vistába is be lett építve.

A szolgáltatásként futó Defender alapértelmezésként engedélyezve van, és az automatikus, ütemezett gyorskeresés is be van kapcsolva. Az alkalmazás kártevő-adatbázisa az internetről a Windows Update szolgáltatás segítségével folyamatosan frissül, de a definíciós fájlok igény szerint akár manuálisan is letölthetők és telepíthetők.

A Windows Defender XP-re telepíthető változata a következő webcímről tölthető le: http://www.microsoft.com/windowsdefender.
A legfrissebb szignatúra fájlok pedig a következő Microsoft tudásbáziscikken keresztül érhetők el: http://support.microsoft.com/?kbid=923159)

A Windows Defender az idő nagy részében a háttérben, a felhasználó megzavarása nélkül fut, jelenlétére csak akkor figyelhetünk fel, ha valamilyen beavatkozás szükséges – ekkor a tálca értesítési területéről egy buboréküzenetet jelenít meg, melyben ismerteti a teendőket.

3.29. ábra: *Nemcsak véd a kémprogramok ellen, hanem a rendszerindítást is befolyásolhatja a Windows Defender*

Az ismert kártevők lefülelésén kívül a Defender valóban átfogó védelmet nyújt a Windows rendszer egészének, így képes a következő eseményeket is detektálni:

- automatikusan induló programok listájának módosulása;
- rendszerkonfiguráció változása;
- Internet Explorer bővítmények telepítése;
- Internet Explorer biztonsági beállítások módosulása;
- szolgáltatások és eszközmeghajtók telepítése, valamint azok konfigurációjának változása;

- alkalmazás-regisztráció (Registry módosulása);
- Windows-bővítmények telepítése.

A Windows Defender része a Software Explorer, mellyel megtekinthetjük a rendszerrel automatikusan induló és az éppen futó alkalmazások biztonsági besorolását, valamint letilthatjuk a nem kívánt startup-programokat. Ha hozzá akarunk járulni a Windows Defender fejlesztéséhez, saját vizsgálat közben született eredményeinket is közzé tehetjük, ha csatlakozunk a Microsoft SpyNet programhoz. A belépés kétszintű, Basic, illetve Advanced tagságot is beállíthatunk. Míg a Basic esetén a Defender csak alapvető információkat küld a Microsoftnak a gépünkön esetlegesen észlelt spyware-ekről, az Advanced tagságot választva minden beállításunkról értesíthetjük a fejlesztőket, például a még be nem sorolt, de általunk biztonságosnak ítélt alkalmazások lenyomatait is feltölti a program – ezzel segítve az adatbázis tökéletesítését.

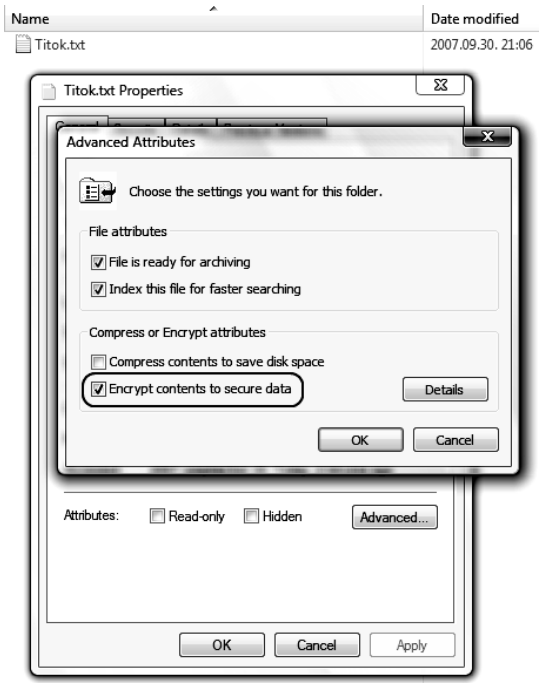
A titkosított fájlrendszer: az EFS

A Windows 2000 óta elérhető titkosított fájlrendszer (EFS = Encrypting File System) az NTFS-fájlrendszer egyik alapszolgáltatása. Segítségével transzparens módon titkosíthatjuk fájljainkat, így azokat a tulajdonos felhasználó a saját profiljába bejelentkezve a szokásos módon elérheti, de a háttértároló tartalma más számítógépbe helyezve – vagy más számítógépről hálózaton keresztül tallózva nem hozzáférhető.

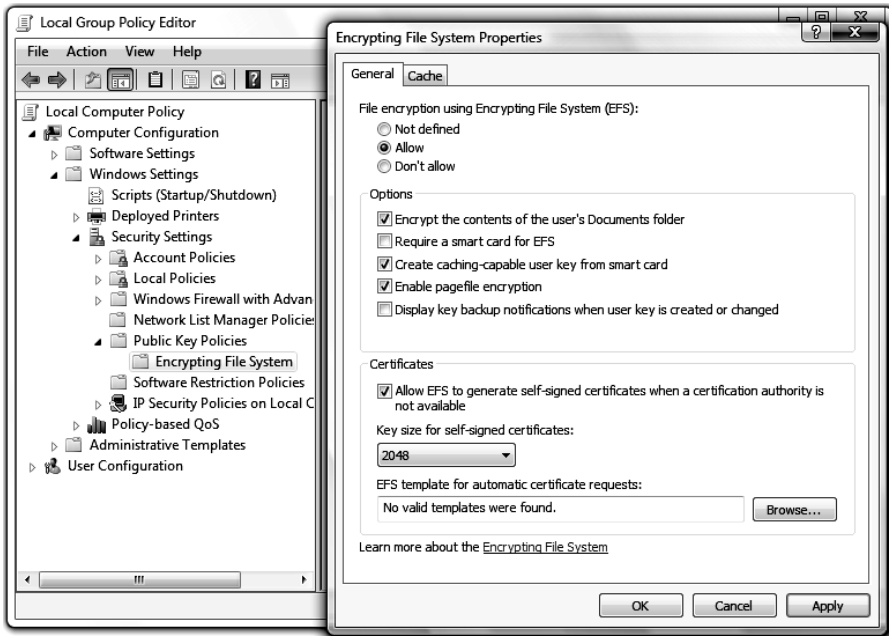
Az EFS-titkosítás érvényesítéséhez egy-egy mappára vagy fájlra mindössze meg kell nyitnunk az objektum tulajdonságlapját, majd az *Advanced* gombra kattintva bejelölnünk az *Encrypt contents to secure data* négyzetet. A titkosított állományok színe a Windows Explorerben alapértelmezésként zöldre változik.

Az egyes fájlokon, vagy teljes mappákon túl a Windows Vista már a lapozófájl titkosítását is lehetővé teszi. Erre azért lehet szükség, mert a lapozófájlban még a rendszer leállítása után is maradhatnak bizalmas adatok, melyek külső eszközökkel kinyerhetők.

Az EFS-sel titkosított adatok visszafejtésére jelenleg nincs lehetőség, hacsak nem rendelkezünk a titkosításhoz használt tanúsítvánnyal. Ezt a tanúsítványt – a titkosítást végző felhasználó profiljába bejelentkezve – a tanúsítványtárból bármikor kiexportálhatjuk, EFS használata esetén pedig erősen ajánlott biztonsági másolatot is tartani belőle arra az esetre, ha az operációs rendszer nem indítható.

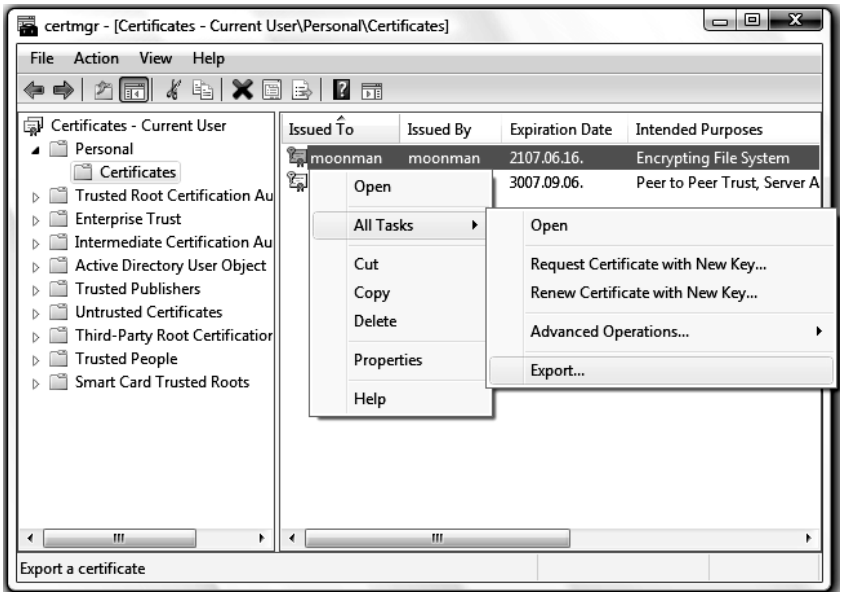


3.30. ábra: *A titkosítás bekapcsolása*



3.31. ábra: *Az EFS házirend-beállítások mennyisége alaposan megnőtt*

Az EFS-tanúsítványt a Certificate Managerből exportálhatjuk ki, melyet a *certmgr.msc* paranccsal indíthatunk. A Personal *(Személyes)* tanúsítványok között jelöljük ki azt, amelynek használati cél mezőjében *(Intended Purposes)* az Encrypting File System bejegyzést találjuk, majd kattintsunk jobb gombbal a tanúsítványra, és az *All Tasks/Export (Összes feladat/Exportálás)* paranccsal mentsük le a fájlt. Ahhoz, hogy egy másik számítógépen, vagy ugyanazon, de esetlegesen újratelepített rendszer esetében hozzáférjünk titkosított adatainkhoz, az imént kimentett tanúsítványfájl importálására van szükség (melyet szintén a Certificate Managerrel végezhetünk el).



3.32. ábra: *Az EFS-tanúsítvány exportálása*

A csoportházirendből igen részletesen konfigurálhatjuk az EFS működését. Lehetőségünk van az EFS teljes tiltására, de beállíthatjuk a felhasználók *Dokumentumok* mappáinak, vagy akár az imént említett lapozófájl automatikus titkosítását, valamint megkövetelhetjük USB SmartCard használatát is.

A Windows Defender és a titkosított fájlrendszer *(Encrypted File System — EFS)*
Ebben a demóban együtt mutatjuk be a Windows Defender kémprogram kereső alkalmazás részleteit, illetve a fájlok/mappák titkosításáért felelős EFS-szolgáltatás megváltozott lehetőségeit.
Fájlnév: I-3-4c-Defender-EFS.avi

BitLocker: a lemezek titkosítása

A felmérések szerint a legtöbb kényes vállalati és személyes információ elveszett vagy ellopott számítógépekről, főként notebookokról jut illetéktelen kezekbe. Éppen ezért egyre inkább elvárás, hogy adataink még a számítógép kikapcsolt állapotában is védve legyenek. A Windows Vista ezt is lehetővé teszi a BitLocker meghajtótitkosítás segítségével. A BitLocker egy vadonatúj technológia, mely a merevlemez tartalmát még a gép szétszerelése és a lemezhez való közvetlen hozzáférés esetén is olvashatatlan adathalmazzá változtatja. Természetesen – mivel az operációs rendszer ilyenkor nem fut – ehhez külső segítségre van szüksége, nevesül a TPM, azaz Trusted Platform Module chipre, vagy egy USB-kulcsra.

A BitLocker két fő funkcióval védi adatainkat: a lemez tartalmának teljes titkosításával (128- vagy 256-bites AES algoritmussal) és a bootfolyamat előtt a kritikus rendszerfájlok integritásának ellenőrzésével. Az operációs rendszer még akkor sem indítható el, ha illetéktelenek valamilyen külső eszközzel esetleg módosítják a betöltést végző komponenseket, így próbálván kiiktatni a titkosítást. A BitLocker a Vista eredeti kiadásában a teljes fájlrendszert – beleértve a lapozó- és hibernációs fájlt is – titkosítja, de csak a rendszermeghajtóra alkalmazható. Ez az állapot várhatóan a Windows Vista első javítócsomagjában változni fog, és az említett korlát végleg megszűnik, azaz a BitLocker titkosítás valamennyi lemezre és partícióra kiterjeszthetővé válik.

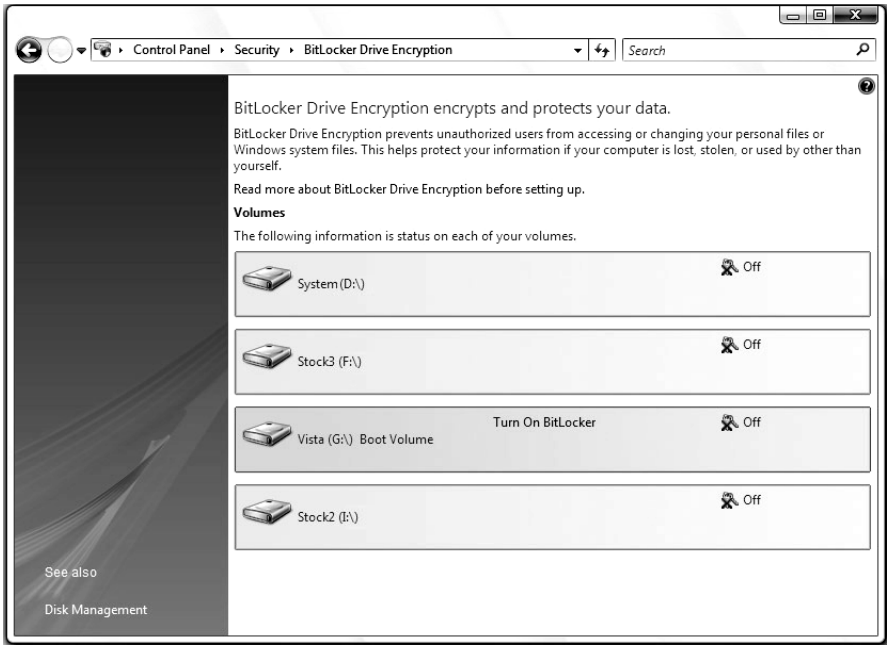
A BitLocker működéséhez az alábbi feltételek szükségesek:

- A BitLocker használatához speciális módon kell particionálni a merevlemezt: a rendszerköteten kívül szükség van egy legalább 1,5 GB méretű, aktív, NTFS fájlrendszert használó partícióra is, melyen a rendszerindító fájlok kapnak helyet – ez a kötet nem kerül titkosításra.
- A számítógép BIOS-ának támogatnia kell az USB-szabványú eszközökről való olvasást és írást még az operációs rendszer betöltődése előtti fázisban.
- Legalább TPM 1.2-es verziójú integrált titkosító chip az alaplapon, vagy egy USB-kulcs.
- Trusted Computing Group (TCG)-szabványt támogató BIOS (TPM használata esetén).

A BitLocker háromféle módon alkalmazható, a következőkben – növekvő biztonsági sorrendben – bemutatjuk a titkosítási eljárás lehetséges konfigurációit.

- **Transzparens mód (TPM chip használata)** – A felhasználónak semmilyen plusz teendője nincs, ha a rendszerindító fájlok érintetlenségéről a TPM modul megbizonyosodott, elindul az operációs rendszer és a felhasználó a szokásos módon bejelentkezhet.
- **USB-kulcs használata** – A felhasználónak még a számítógép indítása előtt csatlakoztatnia kell a titkosítókulcsot tartalmazó USB-eszközt a számítógéphez. Ebben az esetben szükséges, hogy a számítógép még az operációs rendszer betöltése előtt képes legyen kezelni az USB-eszközöket.
- **TPM chip és felhasználószintű hitelesítés együttes használata** – A legbiztonságosabb konfiguráció, ha a TPM modulon kívül a felhasználó birtokában lévő PIN-kód is szükséges az indításhoz. A BitLocker multifaktoros hitelesítéséhez a Windows Vista kétféle módszert támogat: a boot-folyamat előtt a PIN-kód bekérése a felhasználótól, vagy a kiegészítő azonosító USB-kulcsról történő beolvasása.

Mivel a BitLocker technológia elsősorban a vállalati felhasználókat célozza, a meghajtótitkosítást csak a Windows Vista Enterprise és Ultimate változatai támogatják. Ha rendelkezésre áll a megfelelő konfiguráció, a szolgáltatást a *Control Panel/Security/BitLocker Drive Encryption* menüpont alatt kapcsolhatjuk be.



3.33. ábra: *A BitLockert csak a rendszerpartíción használhatjuk (egyelőre)*

A haladó tűzfal és az IPSec-kapcsolatok

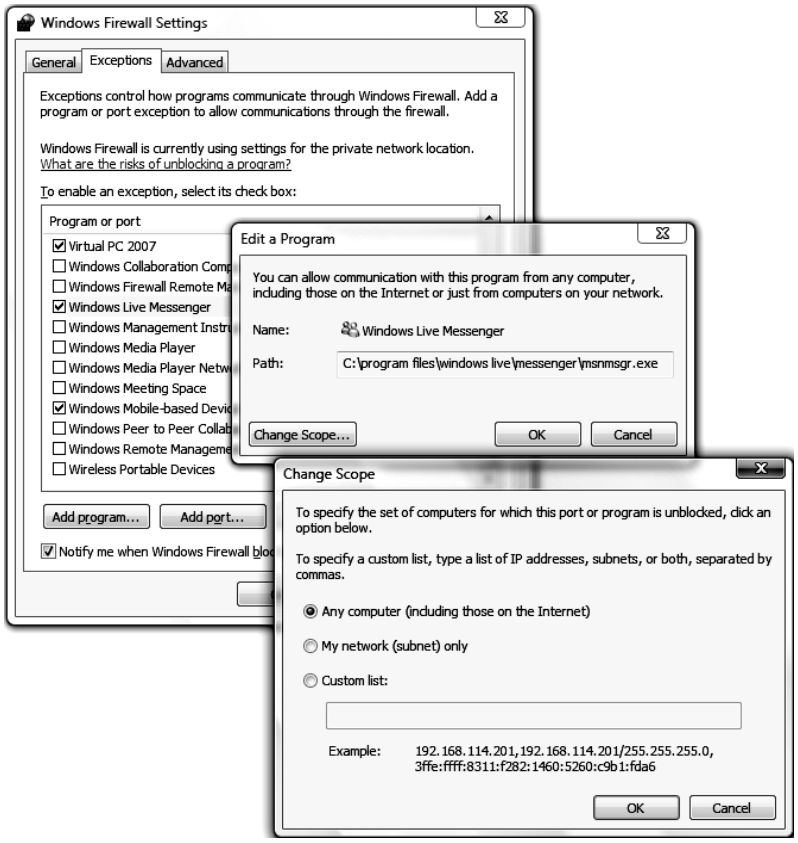
A számítógépes tűzfalak feladata a hálózati interfészeken keresztül folyó forgalom szűrése és – szükség szerint – tiltása. Ezeket a feladatokat különféle szabályok szerint végzik, melyek vagy alapértelmezésként kerülnek beállításra, vagy a felhasználó később határozza meg azokat. A Windows ügyfél operációs rendszerek az XP óta beépített tűzfallal rendelkeznek, mely igazán az XP Service Pack 2-ben vált „nagykorúvá". A Windows Vista viszont egy teljesen új tűzfalat tartalmaz, melynek két arcával is találkozhatunk: az egyszerű, XP-ből már ismerős felülettel és egy rendkívül részletes beállítási lehetőségeket nyújtó, saját MMC-konzollal.

A tűzfal egyszerű felülete a vezérlőpultból egyetlen kattintással elérhető, mindössze a *Security* kategória alatt az *Allow a program through Windows Firewall* hivatkozást kell választanunk. Mint láthatjuk, a kezelőfelület semmit sem változott az XPSP2 óta, a lap első fülén ki-, illetve bekapcsolhatjuk a szolgáltatást (alapértelmezésként be van kapcsolva), valamint egy gombnyomással letilthatjuk a második fülön beállítható kivételszabályokat. Erre akkor lehet szükség, ha valamilyen nem megbízhatónak minősített hálózatra, például egy nyilvános WiFi-hálózatra csatlakozunk.

A második fülön kivételeket képezhetünk saját alkalmazásaink számára, melyeknek a tűzfalon keresztül, saját porton át kell kommunikálniuk a külvilággal. Itt már találhatunk néhány gyárilag konfigurált kivételt olyan Windows-rendszerszolgáltatások számára, mint például a hálózati felderítés, fájl- és nyomtatómegosztás, vagy a távsegítség. Amikor egy program úgynevezett listening portot nyit magának, vagyis bejövő adatokat kíván fogadni, a Windows tűzfal egy kérdést intéz a felhasználó felé, ahol eldönthetjük, hogy engedélyezzük-e a kivételszabály létrehozását. A kérdéssel minden program esetében és minden hálózati profilban csak az első alkalommal találkozunk, a szabály bekonfigurálása után a tűzfal nem kérdez többet.

Kivételszabályt kézzel is megadhatunk, ekkor lehetőségünk van portszám (és hálózati protokoll), illetve alkalmazás szerint létrehozni a bejegyzést. A beállított kivételhez ezek után már csak hatókört kell társítanunk – ez jelentheti csak az alhálózaton, vagy akár minden irányból, így az internet felől történő kapcsolat-fogadását, de megadhatunk egyéni címtartományt is.

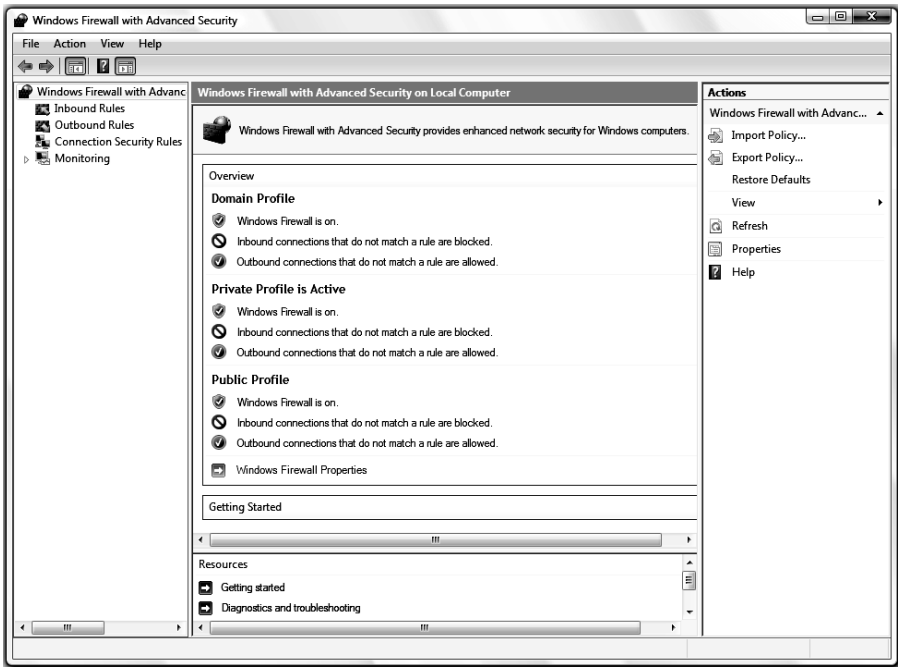
Ha ennél részletesebb beállításokra van szükségünk, a Windows Firewall with Advanced Security *(Fokozott biztonságú Windows tűzfal)* konzolhoz kell fordulnunk, melyet a felügyeleti eszközök között találhatunk. A kezdőlapon egy gyors áttekintést kapunk a tűzfal állapotáról, hálózati profilonként olvashatjuk le a szolgáltatás jellemzőit: fut-e a tűzfal, illetve mely szabályrendszerek szerint vannak tiltva, illetve engedélyezve a kapcsolatok. Alapértelmezésként a tűzfal minden profilban aktív, illetve minden olyan bejövő kapcsolat, mely nem kötődik szabályhoz, tiltás alatt áll.



3.34. ábra: *Az új tűzfal hagyományosan ismerős arca…*

Mivel a Windows Vista alkalmas különféle hálózati szolgáltatások nyújtására is (például web- és FTP-helyek publikálására), illetve egy kártevő program is működtetheti pl. SMTP-kiszolgálóként az operációs rendszerünket, alapvetően szükséges a tűzfal részéről a forgalom kétirányú szűrése. Az új tűzfal ennek megfelelően immár két irányban véd, igaz a kifelé irányuló kapcsolatok szűrése alapértelmezésként ki van kapcsolva, mert a tapasztalatlan otthoni felhasználók számára ez általában szükségtelen és problémákat okozhat – azonban bármikor bekapcsolhatjuk.

A bal oldali sáv legfelső bejegyzésére (*Windows Firewall with Advanced Security – Fokozott biztonságú Windows tűzfal)* jobbkattintva és a tulajdonságlapot megnyitva elérhetjük a tűzfal általános beállításait, itt konfigurálhatjuk be a főlapon is látható paramétereket, valamint a blokkolt kapcsolatok esetén felbukkanó értesítéseket. Több fület is láthatunk, mivel a három hálózati profilnak megfelelően külön-külön határozhatjuk meg a tűzfal működését, egy külön lapon pedig az integrált IPSec-szolgáltatás alapértelmezett beállításait találhatjuk.

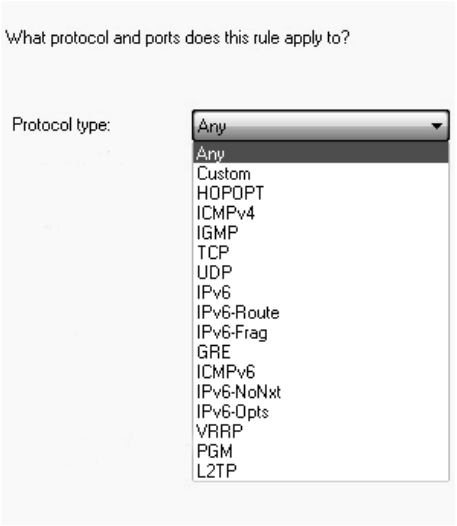


3.35. ábra: *...és a teljesen új MMC konzol, a haladó opciókkal*

A konzol fastruktúrájában találhatók a szabályrendszerek tárolói, illetve az egyéb kapcsolatbiztonsági beállítások, valamint a tűzfal felügyeleti eszközei. Az Inbound Rules *(Bejövő szabályok)* bejegyzésre kattintva előtűnnek a befelé irányuló kapcsolatokra érvényes szabályok. Számos előre definiált bejegyzéssel találkozhatunk itt, ezek közül csak néhány aktív, ezeket a sor előtti zöld ikon jelzi. Egy-egy szabályt kettős kattintással szerkeszthetünk, de a gyári beállításokat érdemes érintetlenül hagyni. Saját szabályt is létrehozhatunk, erre az Action *(Művelet)* menü alatti New Rule... *(Új szabály...)* varázslót használhatjuk, mely végigvezet egy szabály beállításának lépésein.

Mint a tűzfal egyszerűsített vezérlőpultján, itt is lehetőség van program és port szerint is felállítani a szabályt. Pluszként azonban előre definiált szolgáltatásokat (távoli asztal, fájl- és nyomtatómegosztás, hálózati felderítés stb.) is bekonfigurálhatunk – ezekhez előre és eltérő körülményekre legyártott szabályok léteznek – és teljesen egyéni szabály létrehozását is kérhetjük, ahol minden paramétert kézzel kell megadnunk.

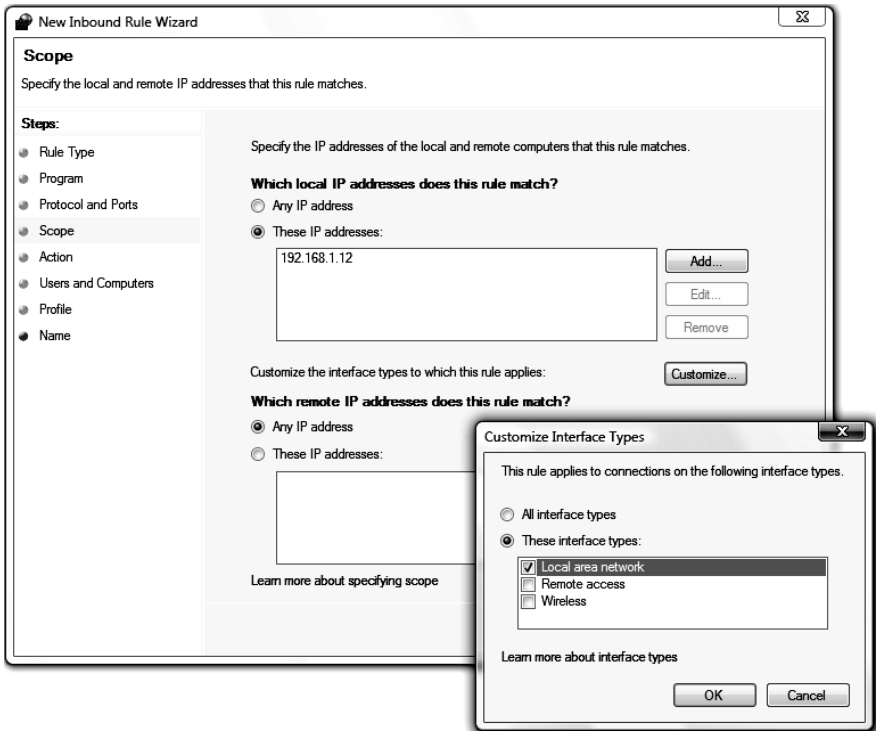
A szabály hatókörét egyes programokra korlátozhatjuk, de egy listából kiválaszthatunk Windows-szolgáltatásokat is. Ha protokoll és port szerint szűrünk, megadhatjuk a protokoll típusát, (illetve számát), a kapcsolathoz használt helyi és távoli portok számát. Ugyanígy a helyi, illetve távoli IP-címeket, sőt akár a hálózati interfészt is megszabhatjuk, melyek a kapcsolatban részt vehetnek, majd azt kell meghatároznunk, hogy a szabály engedélyezze vagy blokkolja az imént beállított paraméterek szerinti kapcsolatokat. Ebben a lépésben beállíthatjuk, hogy a kapcsolat csak akkor legyen engedélyezett, ha az titkosított, tehát biztonságos.



Következő lépésként azokat a hálózati profilokat kell kiválasztanunk, melyekben a tűzfalszabály él, végül egy nevet és egy rövid leírást (opcionális) kell csatolnunk a szabályhoz. Ugyanezzel a varázslóval dolgozunk, amikor kimenő forgalom szabályozását állítjuk be az Outbound Rules *(Kimenő szabályok)* szekcióban.

A Windows tűzfal – mivel MMC konzolból vezérelhető – távoli számítógépről felcsatlakozva is kezelhető, valamint a *netsh* parancssori eszközzel is lekérdezhetjük és megváltoztathatjuk a beállításokat. A tűzfal haladó beállításainak parancssorból történő kezeléséhez használjuk a *netsh advfirewall* utasításcsoportot.

A már említett IPSec olyan nyílt szabványokból álló keretrendszer, amely kriptográfiai biztonsági szolgáltatások segítségével teszi lehetővé a titkosított kommunikációt az IP-protokollt használó hálózatokon. Az IPSec-protokoll két legfontosabb célja, hogy megvédje az IP-csomagok tartalmát, és hogy védelmet nyújtson hálózati támadásokkal szemben a megbízható kommunikáció kikényszerítésével. Az IPSec a titkosításon alapuló védelmi szolgáltatások, a biztonsági protokollok és a dinamikus kulcskezelés alkalmazásával mindkét célnak megfelel. E biztos háttér szolgáltatja azt a hatékonyságot és rugalmasságot, amely a szóló és site-to-site VPN-hálózatok számítógépei, tartományok, és pl. webhelyek közötti biztonságos kommunikációt lehetővé teszi. Sőt, az IPSec a megadott forgalomtípusok fogadásának vagy továbbításának blokkolására is használható.

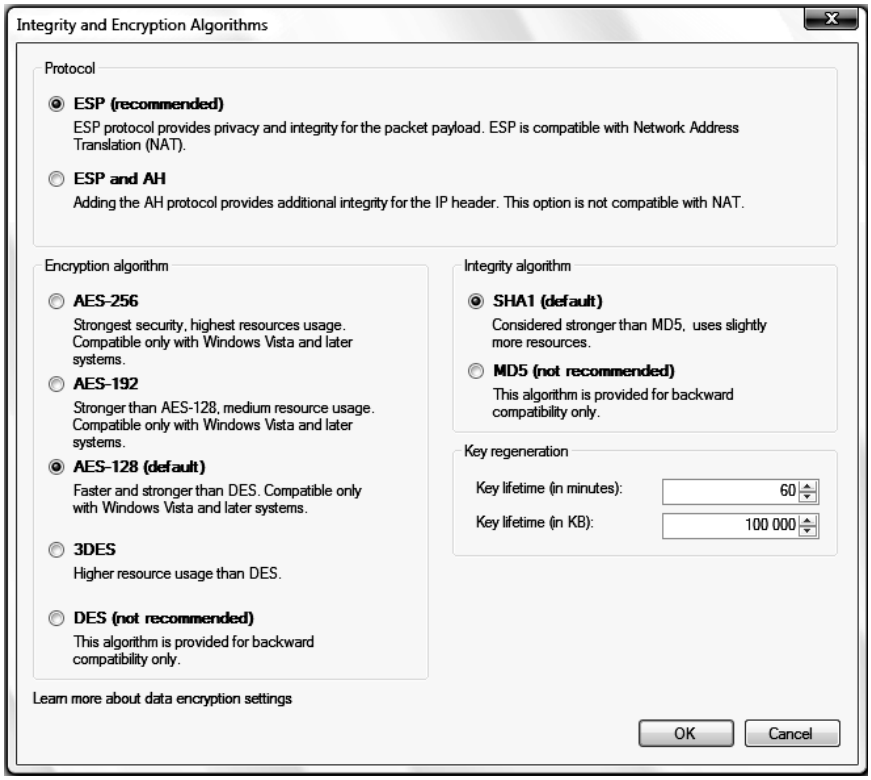


3.36. ábra: *A szabályok akár a hálózati interfész típusától is függhetnek*

Az IPSec-protokoll biztonsági szolgáltatásainak beállításához eddig kizárólag a különböző házirendek voltak használatosak. Az IPSec-házirendek igény szerint alakíthatók, így egy adott számítógépre, alkalmazásra, tartományra vagy az akár az egész vállalatra szabhatók.

A Windows Vistában az IPSec is új ruhába bújt, ezen túl Connection Security Rules *(Kapcsolatbiztonsági szabályok)* néven, a haladó tűzfal MMC-be integrálva is találkozhatunk vele (a csoportházirendből továbbra is definiálhatók IPSec házirendek). De nem csak a ruha új, most már valóban egyszerűvé vált a használat is, azaz nem szükséges elmerülnünk a kriptográfia mélységeibe, ahhoz, hogy bekapcsoljuk két tetszőleges végpont közt az IPSec-et. A haladó beállítások nagyon szépen el vannak rejtve, az alapbeállításokkal viszont eleve biztonságosan, pár kattintással készíthetünk azonnal működő hálózati forgalomtitkosítást.

Kapcsolatbiztonsági szabályokat a hagyományos tűzfalszabályokhoz hasonlóan varázsló segítségével állíthatunk elő, a lehetőségek tárháza bőséges, választhatunk izolációt, kiszolgáló-kiszolgáló kapcsolat beállítását, hitelesítés-mentesítést állíthatunk be, valamint biztonságos átjárót *(tunnel)* hozhatunk létre. Rendelkezésünkre állnak új algoritmusok is, a titkosításhoz AES-128/192/256, a kulcscseréhez ECDH-P 256/384 titkosítást is használhatunk.



3.37. ábra: *Az IPSec titkosítási beállításai*

Az IPSec parancssorból is kezelhető, ehhez a már ismert *netsh* eszközt alkalmazhatjuk. A netsh IPSec kontextusába való belépéshez használjuk a *netsh -c ipsec* parancsot.

A tűzfal MMC-konzol Monitoring *(Figyelés)* tárolóban megtekinthetjük az aktuálisan aktív és működő szabályokat, tűzfal- és kapcsolatbiztonság szerint külön csoportosítva. A Security Associations *(Biztonsági társítások)* bejegyzés alatt az aktív kapcsolatbiztonsági (IPSec) beállítások kerülnek listázásra.

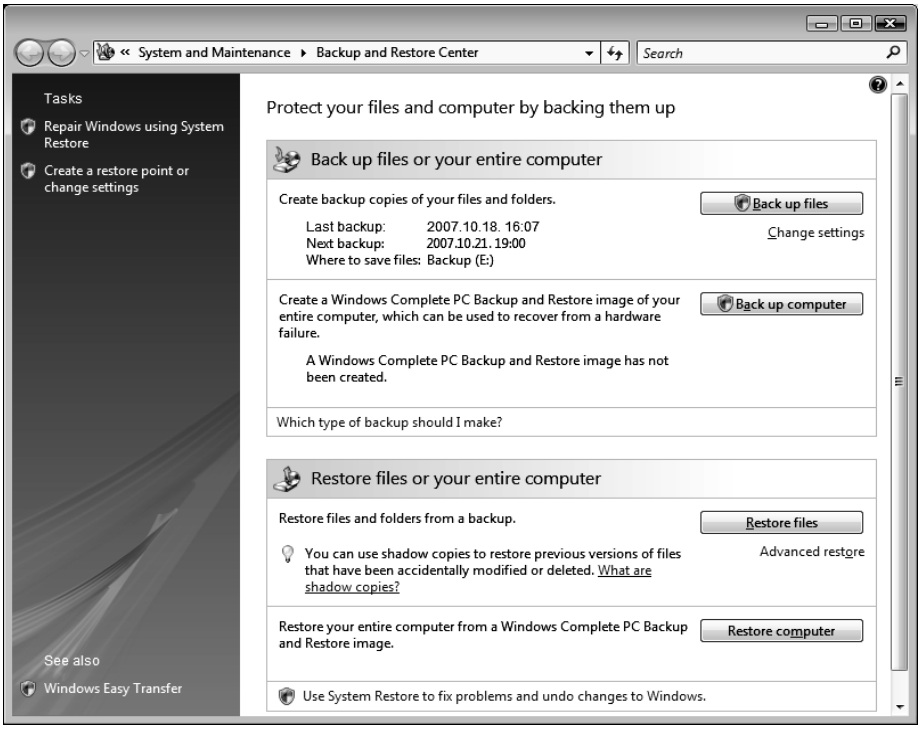
A „két" (valójában csak egy) Windows Vista tűzfal
Ebben az előadásban sor kerül a Windows Vistában integrált tűzfal mindkét arcának bemutatására, a haladó lehetőségeket részletesen kielemezve.
Fájlnév: I-3-4d-Windows-Firewall.avi

Mentés és visszaállítás

A korábbi Windows-verziókkal ellentétben a Vista mentésével és visszaállításával kapcsolatos feladatokat már nem az NTBackup-program, hanem a hangzatos nevű Backup and Restore Center *(A biztonsági mentés és visszaállítás központja), illetve* az innen elindítható Backup Status and Configuration *(Biztonsági mentés állapota és konfigurációja, sdclt.exe)* felületéről végezhetjük el.

! Az NTBackup-program használatával, a kiszolgálók mentésének és visszaállításának kérdéseivel a hatodik fejezetben részletesen fogunk foglalkozni, most csak a Vista speciális lehetőségeivel ismerkedünk meg.

Itt adhatjuk meg az egyes fájlok és mappák, automatikus mentésével, illetve a teljes számítógép disk image *(lemezkép)* alapú mentésével kapcsolatos beállításokat, és innen kezdeményezhetjük az adatok visszaállítását is.



3.38. ábra: *Backup and Restore Center*

A Vista négy különböző lehetőséget nyújt a biztonsági mentések készítésére, ezek mindegyike más módon, és másféle adatok mentésére használható előnyösen. A következőkben áttekintjük az egyes mentési típusokat, és megvizsgáljuk azt is, hogy melyik típus milyen adatok mentésére használható legjobban.

- **Restore points** *(Visszaállítási pontok)* – a rendszerfájlok és a rendszerkonfiguráció mentésére használható, segítségével az operációs rendszer egy korábbi állapotára térhetünk vissza (a felhasználók adataira a visszaállítás nem vonatkozik).
- **Previous Versions** *(Előző verziók)* – a szolgáltatás elsősorban a felhasználók fájljainak mentésére és visszaállítására használható, a mentések automatikusan történnek, a visszaállítási műveleteket pedig maguk a felhasználók kezdeményezhetik. (A szolgáltatás az árnyékmásolatokon alapul, amelynek részletes ismertetése a negyedik fejezetben található.)
- **Create backup copies of yout files and folders** *(Fájlok és mappák biztonsági mentése)* – elsősorban a felhasználók fájljainak mentésére használható automatikus (időzített), illetve kézi indítással.
- **Complete PC backup** *(A teljes számítógép mentése)* – a teljes számítógép lemezkép alapú mentése, ami tartalmazza valamennyi kötet valamennyi adatát, vagyis az összes rendszerfájlt és -beállítást, illetve a felhasználók fájljait is.

A biztonsági másolatok tárolása

A biztonsági mentések típusainak megfelelően alapvetően két különböző módszer áll rendelkezésre a mentéskor keletkező állományok tárolására. A System Restore *(Rendszer-visszaállítás)* és az árnyékmásolatok szolgáltatáshoz kapcsolódó adatok minden esetben a szolgáltatás által védett kötet rejtett részére kerülnek, vagyis például a merevlemez meghibásodása esetén várhatóan nem lesznek elérhetők.

Ezzel ellentétben a fájlokról készített mentések, illetve a teljes számítógép lemezkép alapú mentését tároló fájlok csak önálló tárolóeszközre helyezhetők. A biztonsági mentések a következő adathordozókon tárolhatók:

- Merevlemezek (belső vagy külső).
- Írható DVD- és CD-lemezek. (A program szükség esetén kérni fogja további üres lemezek behelyezését is.)
- Hálózati megosztás (csak fájlokról készített mentés esetén).

A System Restore-szolgáltatás

A System Restore *(Rendszer-visszaállítás)* szolgáltatás segítségével restore pointokat *(visszaállítási pontok)* hozhatunk létre, amelyek lehetővé teszik a rendszer helyreállítását sikertelen frissítések, szoftver- vagy hardvertelepítés, illetve más változtatások után. A következőkben áttekintjük a visszaállítási pontokkal kapcsolatos tudnivalókat és beállítási lehetőségeket.

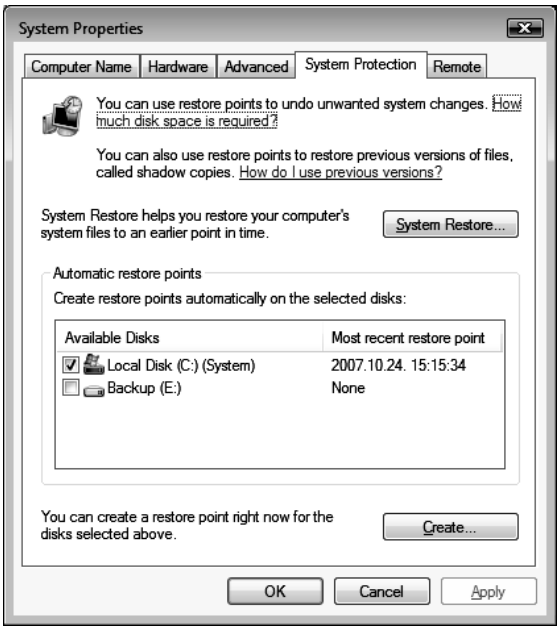
A visszaállítási pont tulajdonképpen a számítógép egy adott kötetének (pontosabban a köteten lévő rendszer- és programfájloknak, illetve a regisztrációs adatbázisnak) lemezre mentett pillanatfelvétele, amelynek segítségével visszaállítható a pillanatfelvétel időpontjának rendszerkonfigurációja. A System Restore-szolgáltatás alapértelmezés szerint napi ütemezéssel automatikusan készíti el a helyreállítási pontokat. A System Restore az adatok mentését kötetenként végzi, vagyis a szolgáltatás az egyes kötetekre engedélyezhető, illetve tiltható. Alapértelmezés szerint a Vista maximálisan az adott kötet területének 15%-át használja a visszaállítási pontok tárolására (a minimálisan szükséges terület 300 MB), és a szolgáltatás a rendszert tartalmazó kötet esetében engedélyezve van.

A *System Restore*-szolgáltatás által mentett adatok az adott kötet *System Volume Information* nevű mappájában tárolódnak. Minden egyes visszaállítási pont külön almappába kerül, amelynek neve tartalmaz egy 32 karakter hosszú egyedi azonosítót (GUID). NTFS-köteteken a mappa nem érhető el a felhasználók számára (még a rendszergazdáknak sem); alapértelmezés szerint egyedül a *System* fiók kap jogot a mappa elérésre. Ha szeretnénk tudni, hogy mennyi helyet foglalnak a *System Restore* által mentett adatok, egy rendszergazda jogosultsággal futó parancssorban adjuk ki a következő parancsot: *vssadmin list shadowstorage*.

Fontos megjegyezni, hogy a System Restore a személyes adatokat (például a felhasználói profil tartalmát) nem menti, így ezeket az esetleges visszaállítás sem fogja érinteni, viszont mivel az árnyékmásolatok (lásd később) készítését is a System Restore engedélyezésével kapcsolhatjuk be, mégis érdemes lehet a szolgáltatást a felhasználói adatokat tartalmazó kötetekre is engedélyezni.

A napi ütemezés mellett természetesen „kézzel” is készíthetünk visszaállítási pontokat (az ábrán lévő Create *(Létrehozás)* gomb megnyomásával), illetve a Vista bizonyos események bekövetkeztekor automatikusan is készít további visszaállítási pontokat. A visszaállítási pont készítését kiváltó események a következők (csökkentett módú rendszerindítás esetén nem készülnek visszaállítási pontok):

- **Program telepítése** – megfelelő telepítőprogram esetén a telepítést megelőzően visszaállítási pont készül. A visszaállítási pont segítségével probléma esetén helyreállíthatjuk a számítógép telepítést megelőző állapotát.



3.39. ábra: *Alapértelmezés szerint a System Restore csak a rendszert tartalmazó kötet változásait figyeli*

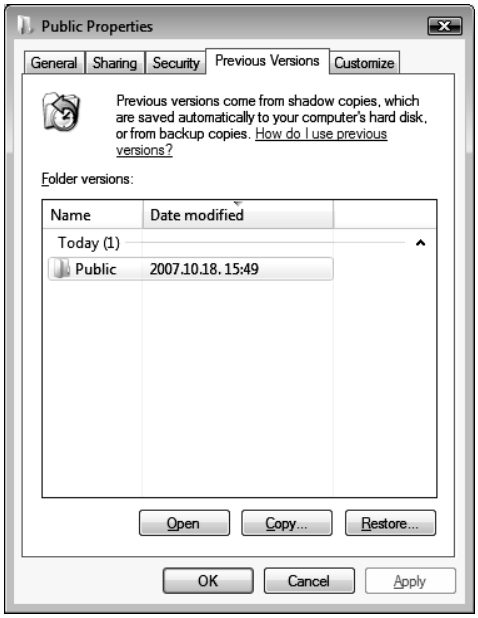
- **Frissítések telepítése** – az automatikus frissítések telepítése előtt is készül visszaállítási pont.
- **Visszaállítási művelet** – visszaállítási pont készül minden visszaállítási pontra történő visszatérés előtt is, így könnyen visszavonhatjuk az elhibázott műveletek hatását.
- **Aláírás nélküli eszközmeghajtó telepítése** – visszaállítási pont készül az aláíratlan, illetve nem minősített eszközmeghajtók telepítése előtt. (A minősített meghajtók korábbi állapotának visszaállítása a Device Manager *(Eszközkezelő)* Driver Rollback *(Az eszközmeghajtó visszaállítása)* műveletével lehetséges.)
- **Mentésből való visszaállítás** – visszaállítási pont készül, ha a Vista beépített mentőszoftverének segítségével fájlokat állítunk vissza.

Problémát okozhat, ha a Windows Vista-rendszer mellett Windows XP is telepítve van a számítógépen. Ebben az esetben a Windows XP indításakor a Vista által mentett valamennyi visszaállítási pont (az árnyékmásolatokkal együtt) megsemmisül. A jelenségnek oka az, hogy mivel a Windows XP nem ismeri a Vista által létrehozott visszaállítási pontok formátumát, azt feltételezi, hogy azok sérültek, így egyszerűen törli őket, majd létrehozza a saját visszaállítási pontjait.

A Previous Versions-szolgáltatás

A Previous Versions *(Előző verziók)* szolgáltatás a sérült, illetve véletlenül módosított vagy törölt fájlok egyszerű, a felhasználók által kezelhető visszaállítási lehetőségét biztosítja. Egy fájl vagy mappa előző verziója származhat a Vista beépített mentőszoftverével létrehozott mentési fájlból, vagy árnyékmásolatból, amelyek a visszaállítási pontok részeként alapértelmezés szerint naponta egyszer kerülnek mentésre (csak változás esetén).

Az árnyékmásolat-szolgáltatás a Windows Server 2003 esetében is létezik, erről részletes leírás található a negyedik fejezetben. A Windows Server 2003 esetén azonban az előző verziók csak az árnyékmásolattal védett kötet megosztott mappáinak elérésekor állnak rendelkezésre. A Vista újdonsága, hogy az árnyékmásolatok, és így a fájlok és mappák előző verziói helyi kötetek esetében is elérhetők és használhatók.



3.40. ábra: *Az árnyékmásolat szolgáltatás helyi meghajtókra is használható a Vistában*

Az árnyékmásolatokat a rendszer a visszaállítási pont részeként, az ott megadott paramétereknek megfelelően menti. Ha a System Restore szolgáltatás engedélyezve van (a szolgáltatás alapértelmezés szerint csak a rendszert tartalmazó kötetet védi), akkor a kötet megváltozott fájljairól naponta egy árnyékmásolat készül (természetesen a nem módosított fájlokról nem). Ha több kötetet is szeretnénk védeni az árnyékmásolatok segítségével, azokon is engedélyeznünk kell a System Restore-szolgáltatást.

Az árnyékmásolatok használatával kapcsolatban mindenképpen figyelembe kell vennünk az alábbi szempontokat:

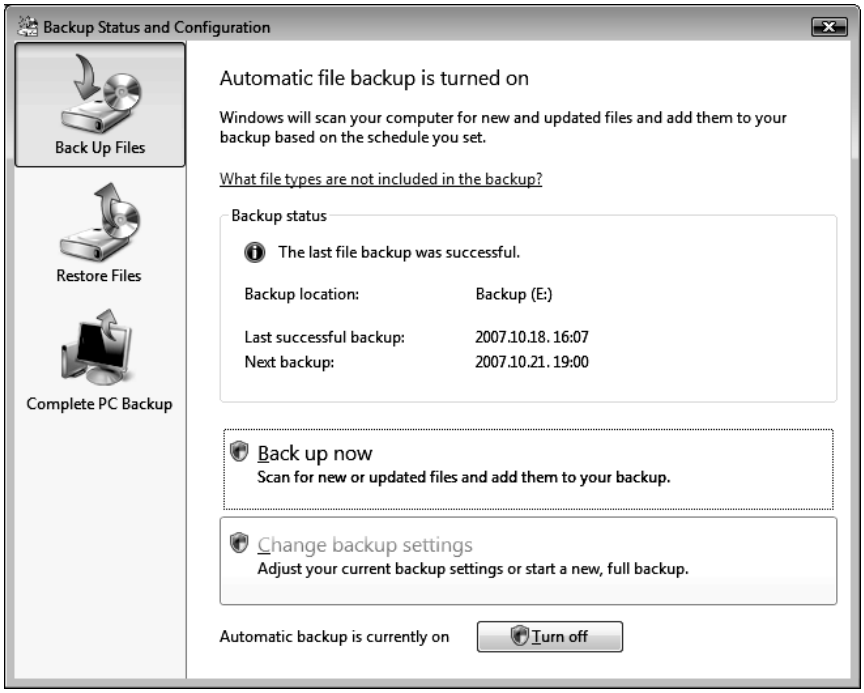
- Az árnyékmásolatok élettartama korlátozott. Alapértelmezés szerint a kötet 15%-a áll rendelkezésre, erre a célra, ha ezt elérjük, a további árnyékmásolatok elkezdik felülírni a legrégebben készült példányokat.
- Árnyékmásolat csak a fájlok, illetve mappák megváltoztatásakor készülnek. Ha egy adott fájl már hosszú idő óta változatlan, akkor elképzelhető, hogy egyáltalán nem lesznek árnyékmásolatai (bár ebben az esetben nincs is szükség rájuk).
- Amint már említettük, ha a számítógépen más operációs rendszert (Windows XP-t) indítunk el, akkor valamennyi árnyékmásolat és a visszaállítási pontok is törlődni fognak.

A rendelkezésre álló előző verziók megtekintéséhez kattintsunk a fájlra, illetve mappára az egér jobb gombjával, és válasszuk a Restore Previous Versions *(Korábbi verziók visszaállítása)* menüpontot.

Az előző verziók *(Previous Versions)* használata
Ebben a demóban bemutatjuk a Vistába immár alapértelmezésben integrált Previous Versions szolgáltatás igencsak kellemes előnyeit.
Fájlnév: I-3-5a-Previous-Versions.avi

Fájlok és mappák mentése

A fájlalapú mentés segítségégével a felhasználók személyes fájljainak mentését végezhetjük el, ez a módszer programok, illetve beállítások mentésére nem használható. A mentési fájlból önálló fájlokat és mappákat is visszaállíthatunk, de például a merevlemez meghibásodása esetén először fel kell telepítenünk az operációs rendszert és valamennyi programot. A mentés a beállított ütemezés szerint történik, de az időzítésen kívül csak a mentési helyet és a mentendő fájlok típusát határozhatjuk meg.



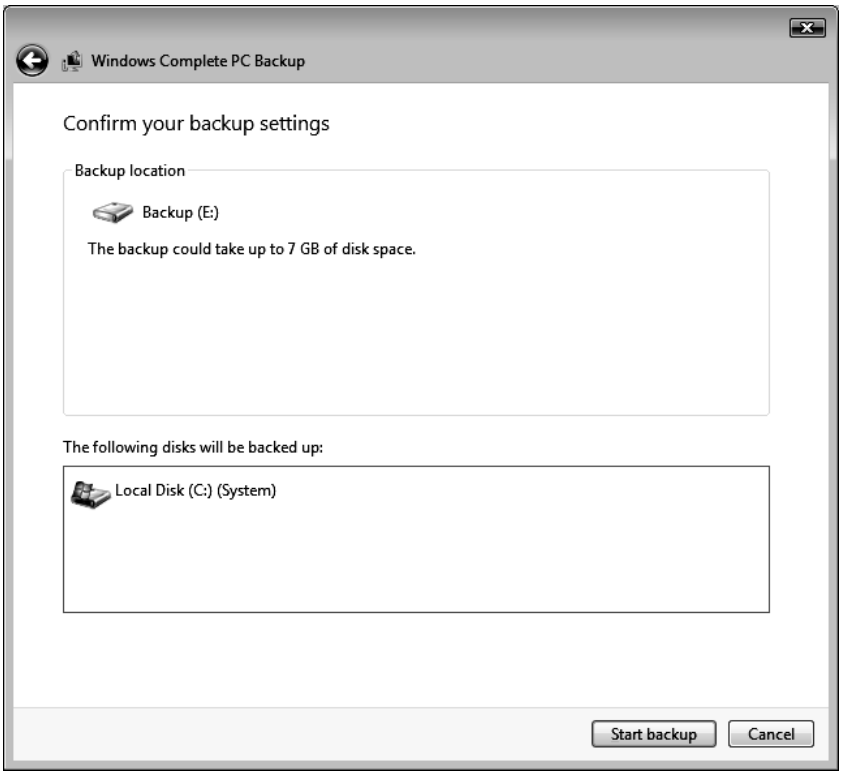
3.41. ábra: *A Vista beépített mentőszoftvere automatikusan menti a felhasználók fájljait*

Complete PC Backup

A teljes számítógép mentése azt jelenti, hogy a számítógép kijelölt köteteiről (a rendszerkötetről mindenképpen) lemezkép *(disk image)* alapú másolatot készítünk. A lemezkép tartalmazza az adott kötet valamennyi adatát, a rendszerfájlokat és beállításokat, valamint a felhasználók fájljait is. A mentési fájl (vagyis a lemezkép) mérete nagyjából meg fog egyezni az összes elmentett adat eredeti méretével.

A lemezképek formátuma a Virtual PC (és a Virtual Server) által is használt *.vhd* (virtual hard disk) formátum, vagyis azok akár egy virtuális gép alá is becsatolhatók.

Mielőtt a mentést elvégeznénk, célszerű megkeresni és kijavítani a kötet esetleges hibáit (*chkdsk*), és töredezettségmentesíteni a kötetet. Ha a mentést második merevlemezre szeretnénk elvégezni, NTFS fájlrendszerrel kell megformáznunk azt (tömörített kötetre nem helyezhetjük a mentési fájlt).



3.42. ábra: *A rendszerkötet lemezkép alapú mentése második merevlemezre*

A teljes számítógép mentése csak teljes kötetekre vonatkozhat, egyedi fájlok vagy mappák kiválasztására nincs lehetőség, így aztán a mentés elvégzése is meglehetősen egyszerű: csak a célhelyet kell megadnunk és ki kell választanunk a mentendő köteteket.

A számítógép visszaállítását elvégezhetjük a Backup and Restore Center felületéről, de nem induló rendszer esetén ez az út természetesen nem járható. Ebben az esetben a visszaállításhoz a Vista telepítőlemezéről kell elindítanunk a számítógépet, de a szokásos telepítés helyett válasszuk a Repair Your Computer *(Számítógép javítása)* hivatkozást, majd a Windows Complete PC Restore *(Windows Complete PC Visszaállítás)* opciót.

Mentés és visszaállítás
Ez a részletes előadás a Vista fájlokat és mappákat érintő mentőeszközével, illetve a speciális komplett lemezkötet mentés szolgáltatással foglalkozik.
Fájlnév: I-3-5b-Mentes-visszallitas.avi