Debreceni Egyetem
Informatika Kar

Számítógépes biztonság MS platformon

Témavezető:
Dr. Krausz Tamás
számítástechnikai
tudományos munkatárs

Készítette:
Szlezák Gergely
programozó
matematikus

Debrecen
2007

Tartalomjegyzék

1. Bevezetés

A számítógépeink és a számítógépes adataink védelme egyre növekvő jelentőséggel bír, ennek megfelelően egyre nagyobb érdeklődés mutatkozik a számítógép-biztonság iránt is. A védelem jelentősége lényegesen megnőtt a hálózatok megjelenésével, a védekezés összetettebbé és bonyolultabbá vált, s a felhasználóknak ugyanakkor eddig nem ismert veszélyforrásokkal kell szembenézniük. A biztonság alapja a jó menedzsment, a megbízható és kellően integrált hardver és szoftver, a szakképzettség és a kulturált használat.

Ha azt halljuk, hogy biztonság, mindenki másra gondol először (természetesen most számítástechnikai vonatkozásban gondolkozunk). Rengeteg értelmezése van, érthetünk alatta titkosítást, adatbiztonságot, fizikai biztonságot, szolgáltatás biztonságát vagy akár a rendelkezésre állást is. Az Internet biztonság és az adatbiztonság az elmúlt években vált igazán divatos fogalommá, a hálózati biztonság egyes területeken pedig mára alapvető fontosságú. Például manapság a vállalatok a legféltettebb üzleti titkaikat is elektronikus formában tárolják, ügyfelek százainak-ezreinek adatait tartják nyilván, így előfordul, hogy már törvényileg kötelezik őket a védekezésre, a működés naplózására. Persze nem kell az adott vállalatnak egy multinacionális cégnek lennie, ma már a kisvállalkozások is sokkal több figyelmet fordítanak a biztonsági kérdésekre.

A számítógépes biztonság alatt szűkebb értelemben az adataink illetéktelen hozzáféréstől való védelmét értjük. Tágabb értelemben viszont ide tartozik az elérhetőség és megbízhatóság tárgyköre is. Megbízhatóság alatt leginkább azt értjük, hogy mennyire lehetünk biztosak rendszerünk megbízható működésében. Ez hardveres és szoftveres üzembiztonságot is magában hordoz, valamint az események nyomon követési rendszerét is.

Ahhoz, hogy a megfelelő védelmet ki tudjuk építeni, tisztában kell lennünk a lehetséges veszélyforrásokkal. A szinte mindig jelen lévő fizikai sebezhetőség mellett ott lehetnek az emberi támadók és a programozott kórokozók. Ezeket a 2. és 3. fejezet részletesen bemutatja.

Ne gondoljuk azonban azt, hogy ha nem használunk Windows-os rendszereket, akkor máris biztonságban vagyunk, ugyanis ez a probléma ugyanúgy érinti például a Linuxos platformot is. Elterjedtsége még messze elmarad a Microsoft termékeitől, de már most egyre több Linuxra írt vírus jelenik Egyesek már a Linux vírusok globális járványát látják a láthatáron. A biztonság növelhető, ha gépeinket (lehetőség szerint) lekapcsoljuk az Internetről, használjuk a megfelelő biztonsági megoldásokat vagy rendszereinket hozzáértő rendszergazdákra bízzuk. De talán ezt az oktatásba is komolyabban be lehetne építeni és a felnövő új generációk már tisztában lennének a veszélyekkel és a védekezés lehetőségeivel.

A szakdolgozat kitér a legismertebb fizikai és szoftveres megoldásokra, valamint technológiákra. Ezeken kívül betekintést ad a Windows Vista biztonsági szempontból fontos újdonságaiba.

2. Fizikai biztonság

Itt kell megemlítenünk a fizikai hozzáférés, lopás, elemi károk, a használat, üzemeltetés során felmerülő problémák együttesét. Ezek lehetnek tőlünk független események, de akár szándékosak is. A felsorolt történések nagyban veszélyeztetik hardver-eszközeink biztonságát.

A felsorolás első felének megoldására rengeteg lehetőség van (sokszor elég drága), melyeket érdemes betartani és megfontolni. Hálózatok, számítóközpontok esetén a szervereket célszerű egy elkülönített helyiségben tárolni, mely jól zárható. Ezzel jól le tudjuk korlátozni a fizikai hozzáférés lehetőségét. A helyiség legyen klimatizált, tűzjelzővel és tűzoltó készülékkel felszerelt, beriasztózott. Jó, ha van áramtalanító főkapcsoló és elég hely az eszközöknek és a szabad mozgásnak. Érdemes beszerezni szünetmentes tápegységeket is és erről üzemeltetni a szervereket. Használjunk minél jobb minőségű kábeleket, ezzel nem érdemes spórolni. A szerverszobán kívüli eszközök elzárhatóságáról is gondoskodni kell. Persze, hogy mit alkalmazunk ezekből a megoldásokból, a pénztárcánk határozza meg, de ne felejtsük el, hogy a biztonság alapjai itt kezdődnek és egy esetleges kár költségei jóval nagyobbak lesznek, mint amit a védelem kiépítésére fektetünk.

A többi felsorolt veszélyre megoldást jelenthet a kimentés vagy valamilyen hardveres technológia alkalmazása, mint például a RAID.

2.1. Mentés

Fontos adataink biztonságos helyre mentése általában addig nem tűnik olyan fontosnak, míg egyszer rosszul nem jár az ember. Olyankor persze már késő, ezért jó előre gondolkodni és megtenni azt bizonyos időközönként. Erre a legjobb módszer kiírni az adatokat CD-re vagy DVD-re és eltárolni a lemezt egy biztonságos (nem hozzáférhető, tűzbiztos) helyre. Az adatmentés korlátozódhat a fontosabb felhasználói fájlokra, de akár az egész rendszer mentését is magában foglalhatja.

2.2. RAID

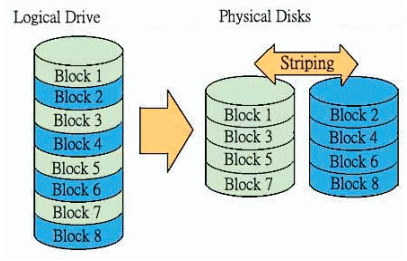
Manapság egyre elterjedtebb és rendkívül megbízható fizikai megoldás. A Microsoft Windows NT alapú rendszerek a fizikai mellett a szoftveres RAID-hez is adnak támogatást. Főleg szerverek esetében használatos, de kezd megjelenni munkaállomásokon is. Rendszerint speciális RAID kontroller kártyát használnak, jellemzően SCSI diszkekkel, de léteznek IDE RAID csatolók is.

A RAID a Redundant Array of Inexpensive/Independent Disks rövidítése. Először az Inexpensive volt használatos, mivel régebben a drága lemezek felváltása volt inkább a cél. Azonban később a merevlemezek ára annyira lecsökkent, hogy más szempontok kerültek előtérbe és felváltotta az Independent szó.

A RAID alkalmazásával növelhető a rendszer teljesítménye és hibatűrése. Más-más rendszerekben viszont eltérhetnek a megvalósítandó célok, ezért több szintre bontották a RAID-et, melyek eltérő jellemzőkkel rendelkeznek.

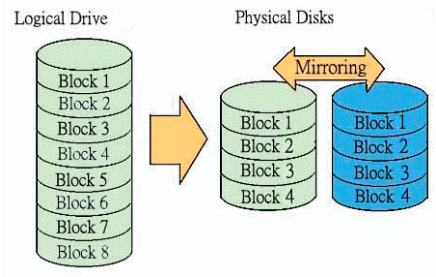
RAID 0 = darabolás (striping):

Darabolt lemezek tömbjét kezeli. Elsősorban teljesítménynövelésre használják, de adatvesztéstől nem véd.



RAID 1 = tükrözés (mirroring):

Minden adatot teljes egészében kétszer tárol, ezzel nagyban megnöveli a biztonságot. A teljesítményre viszont nincs hatással és költséges is.



RAID 2:

Bitcsoportok *stripe set* kezelését végzi hibajavítással. A bitcsoportokat különböző lemezekre osztja szét és tárolja. Egy esetleges sérülés esetén az adatok helyreállíthatóak valamilyen hibajavító kódolás (pl. Hamming kód) segítségével.

RAID 3 = paritásos darabolás:

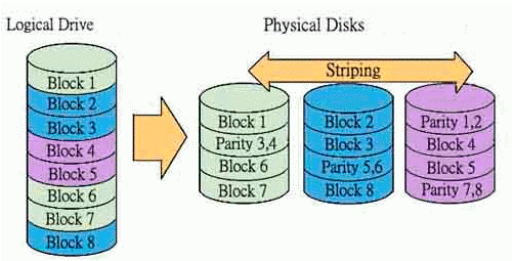
A paritás bitek külön, dedikált lemezre kerülnek. Két vagy több lemezdarabolást kombinál egy paritás meghajtóval. Biztonságos és gyors is, mivel a lemezek párhuzamosan használhatóak. Egy hátránya, hogy legalább 3 lemezt igényel.

RAID 4:

Hasonló a RAID 3-hoz, csak a lemezek menedzselése függetlenül történik.

RAID 5:

A leggyakrabban alkalmazott megoldás. Osztott paritást használ, azaz feldarabolja az adatokat és a paritás biteket, de ezeket két lemezenként tárolja egy harmadikon. Így teljesítmény szempontjából is megfelelő és biztonságos is.

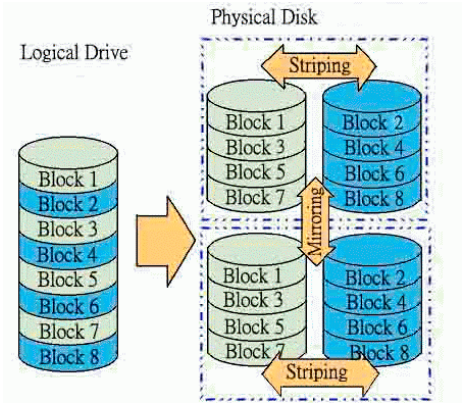


RAID 6:

A legmegbízhatóbb megoldás, de még nincs elterjedve. Annyiban különbözik a RAID 5-től, hogy két különböző paritásképzést használ vagy ugyanazt, de az adatok csoportjainak átlapolásával. A paritás adatokat legalább két, független paritás lemezen tárolja.

RAID 0+1:

Ez is elterjedt megoldás, a RAID 0 és a RAID 1 tulajdonságait egyesíti.



Az, hogy melyik szintjét választjuk a technológiának, azt a saját, egyedi igényeink határozzák meg. A megbízhatóság-teljesítmény-költség hármast kell körültekintően átgondolni.

A RAID alkalmazása sokszor azt a téves biztonságérzetet kelti, hogy a rendszerünk már védett, nem történhet semmi. Pedig vannak helyzetek, amikor még a RAID sem véd meg:

- Áramszünet – félbemarad az írás folyamata, így inkonzisztens lesz az adat
- Lemez meghibásodása – ezt azonnal ki kell javítani, mert ha egy lemez kiesése még nem mindig okoz adatvesztést, a másodiké már biztosan
- Egyszerre több lemez-meghibásodás – ekkor még a RAID sem képes biztosítani az adat-visszaállítást
- Emberi tévedések, szándékos károkozás
- Számítógép meghibásodása, elemi csapások

2.3. Hardveres megoldások

A hardverből megvalósítható védelem például hardverkulcs segítségével történik. A hardverkulcs lehet olyan eszköz, amely hardveresen segíti a hitelesítést. Ezen eszközök valamilyen titkosítási algoritmuson alapulnak. A kulcs tárolja a „jelszót”. Biztonságosabb és kényelmesebb, mint megjegyezni jelszavainkat, de azért vannak vele problémák is.

Előnye tehát, hogy biztonságosabb, nem lehet lemásolni és ha valaki mégis hozzájut, akkor könnyű észrevenni, mivel csak 1 példány van belőle.

Hátránya viszont, hogy elvesztés esetén, ha nem vesszük ezt időben észre, a kulccsal hozzáférése lesz egy nem kívánt személynek a védett tartalmakhoz. Ezt szokás kivédeni olyan módszerrel, hogy kombinálják a hardveres kulcsot a szokványos jelszóval, így egy belépéshez mindkettővel rendelkeznünk kell. Sajnos az sem elhanyagolható, hogy egy ez plusz eszköz, így plusz kiadással is jár, főleg ha sok alkalmazottnak kell kiosztani ilyet.

Példaként megemlíthetjük a Smart Card[1] technológiát vagy az Aladdin cég hardveres megoldásait.

Egy másik megoldás kicsit más oldalról közelíti meg a dolgot és szorosan kapcsolódik a szoftveres veszélyekhez. A legújabb AMD és Intel processzorok ugyanis megnehezítik a kártevők életét. Már a processzorba építve megtalálható olyan funkció (Execution Protection), amely konkrétan a puffer-túlcsordulásos sebezhetőségek ellen ad védelmet.

Léteznek olyan kártyás megoldások, ahol egy új kártyát építve a gépbe kapunk biztonsági funkciókat. Véd a szándékos és a véletlen károkozással szemben is. Képes letiltani a beállítások megváltoztatásának, adatok törlésének lehetőségét. Kezeli az áramszünetből adódó problémákat. Az egyéb funkciók közé tartozik például, hogy a jogosulatlanul feltelepített programok újraindítás után eltűnnek.

[1] Bankkártya méretű plasztik kártya, melyen elhelyeztek egy integrált áramkörös chippet, mely kisebb mennyiségű információ tárolására képes. Ilyet használnak a bankok, a kártyás beléptető rendszerek és a felsőoktatási diákigazolványok is ilyenek.

3. Szoftveres biztonság

A Microsoft platform régebben nem számított valami megbízhatónak és manapság is sokan „öngyilkosságnak” tartják az ilyen rendszerekre építkezést. Azonban ahogy telt az idő, újabb és újabb operációs rendszer-generációk jelentek meg, melyek nagyságrendekkel fejlettebbek voltak elődjüknél. Egy 2007 elején megjelent Symantec biztonsági jelentés összehasonlította a legismertebb platformokat hibáik száma alapján. Érdekesség, hogy a 2006 második félévében felfedezett sebezhetőségek számát illetően a Windows szerepelt a legjobban, ugyanis „csak” 39 sérülékenységgel küzdött, míg a Mac OS X 43-mal, a Red Hat pedig 208-cal. Ráadásul a Microsoft volt a leggyorsabb a hibajavítások kiadását illetően is. Persze ha ennyi lenne, nem is lenne semmi gond. Ez a jó eredmény viszont elhalványul, ha megnézzük, hogy a sérülékenységek nagy része kritikus besorolású, míg a többi platform esetében ilyet alig találunk. Sajnos a Microsoft operációs rendszerének vesztét éppen annak elterjedtsége okozza. Mivel legtöbben még mindig Windows rendszereket használnak, ez válik leggyakrabban a támadók célpontjává, Windows alá készülnek el leggyorsabban a réseket kihasználó ártó szándékú kódok. Természetesen megvannak a módszerek arra, hogy az előbbiek ellenére maximalizáljuk rendszerünk védelmét.

3.1. Az operációs rendszer és a fájlrendszer

A szoftveres biztonság az operációs rendszernél és a fájlrendszernél kezdődik. E két fogalom szorosan összefügg. Lehet a fájlrendszer biztonságos, ha az operációs rendszer nem támogatja annak lehetőségeit. És fordítva is igaz, hiába vannak az operációs rendszernek biztonsági összetevői, ha a fájlrendszer alkalmatlan azok használatára. Sokáig a FAT rendszerek voltak elterjedtek, nagy előnyének lehetett megemlíteni a gyorsaságát, persze ez csak kisebb kötetek esetén volt így. A sebessége nagymértékben csökken egyre nagyobb cluster-méret esetén. Az NT bizonyos verziói támogatták az OS/2 fájlrendszerét, a HPFS-t is. Ez biztonság szempontjából sokkal fejlettebb, de kis köteteken pazarló, a mai nagy köteteken pedig már nem olyan

hatékony. Az igazi áttörést az NTFS fájlrendszer hozta, melyet az NT alapú rendszerek használhatnak. Rengeteg biztonsági funkciót építettek bele, hátránya szinte nincs is. Esetleg az, hogy a sok biztonsági információ és bejegyzés több lemezterületet foglal le, de ez a mai merevlemez-kapacitások mellett elhanyagolható; valamint az, hogy a régebbi Windows rendszerek vagy más operációs rendszerek legfeljebb olvasni tudják. Az NTFS-ről egy bővebb leírás a 4. fejezetben található.

3.2. Active Directory

Az Active Directory a Windows 2000 új címtáraként jelent meg. Nagyon összetett és szétterjedő struktúrája miatt csak megemlítés szintjén fog szerepelni.
Ez egy olyan nyilvántartás, mely egy elosztott rendszer erőforrásainak (felhasználói adatok, alkalmazások, számítógépek, nyomtatók, stb.) információit egy központi helyen tárolja. Minden egy helyen van, így kevesebb a támadási pont, igen biztonságos. Segít a felhasználó-kezelés hatékonyságának, biztonságának és kényelmének növelésében, a szoftver és hardver üzemeltetési költségeinek csökkentésében.
Jellemzői:

- Hierarchikus, kiterjeszthető névtér
- Több mesterpéldányt használó replikáció
- Szervezeti szintű, globális katalógus
- X.500 szabványon alapul
- DNS-alapú erőforrás-elérés
- LDAP v3.0 alapú adatkezelés
- Integráció a védelmi alrendszerrel, a hálózattal és a kezelőfelülettel
- Nagy teljesítményű adatbázis (skálázható, indexelt, partícionált, megbízható)
- Nyilvános séma objektum
- Hatékony replikáció

3.3. Programozott kórokozók

A veszélyes vagy káros kódok írása már jó régen foglalkoztatja az embereket. Már a ’80-as években elkészültek az első ilyen programok. Persze az igazi térnyerésükhöz kellett az, hogy a számítógép széles körben elterjedjen és minél több ember számára hozzáférhető legyen. A technika fejlődése sok új fajt hozott létre és volt, amit kipusztított (szinte teljesen eltűntek a boot-vírusok). Ezen programok közös jellemzője a reprodukció, a terjeszkedés és a károkozás. Mondjunk pár szót a fajtáiról.

Vírus:
Általános megfogalmazás, hogy olyan programkód, mely képes magát reprodukálni, de önmagában életképtelen, szüksége van egy gazdaprogramra, melyet megfertőz. Általában csak a fertőzött program végrehajtásakor aktivizálódik és kezdi meg működését (kivéve például a boot-vírus, mely a rendszer betöltődésekor már aktív). Speciális változata a makró-vírus, mely nem operációs rendszer függő, hanem egy bizonyos szoftverhez kötődik. Annak makrói közé furakodik be és a szoftverhez kötődő dokumentum megnyitásakor fut le. A Microsoft Office programcsaládhoz rengeteg ilyen típusú vírus jelent meg, de manapság inkább eltűnőben vannak.

Trójai faló:
Olyan kód, program, mely más programba van rejtve. Hasznos programnak van álcázva vagy egy ismert program módosított változata.

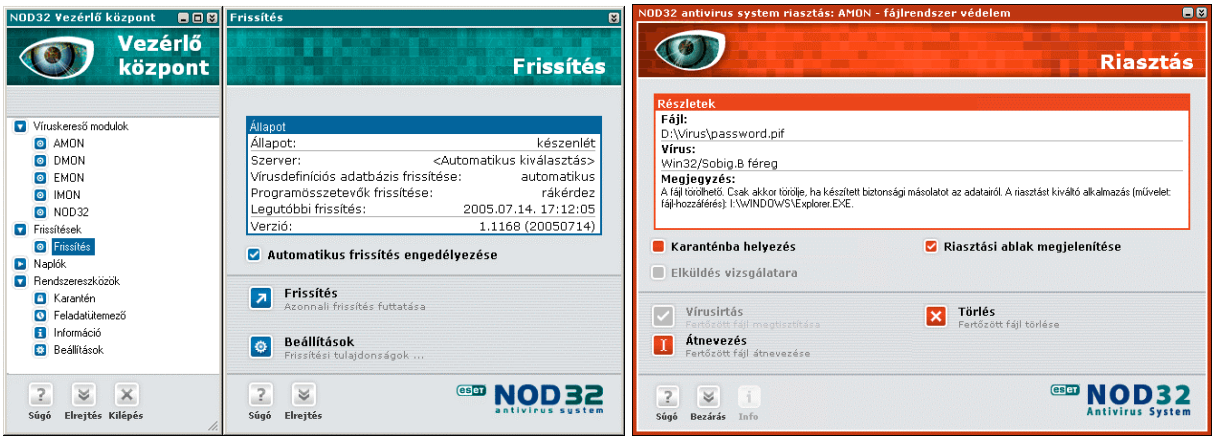
Féreg:
Önálló program, mely kívülről próbál meg beszivárogni a rendszerbe és siker esetén fejti ki hatását. Az Internet térnyerésével ez a fertőzési forma ma az egyik legveszélyesebb és leggyorsabban terjedő fenyegetés. A legismertebb fertőzési hullám a közelmúltban történt a Blaster nevezetű féreg által. Rekord gyorsasággal jutott be több millió számítógépre a világon és több 100 millió dollár kárt okozott világszerte.

Azért meg lehet említeni azokat a férgeket, melyek nem rossz szándékkal készültek. Ezek behatolnak a sérülékeny rendszerekbe és kijavítják azok biztonsági réseit.

Kiskapu (csapóajtó):
Manapság ez is egy elterjedt megoldás. Vírus, faló vagy féreg is létrehozhat rendszerükön ilyen kiskapukat. Ezzel az a célja a kód írójának, hogy később bármikor visszatérhet és a kapun keresztül bejutva információt szerezhet, kárt okozhat vagy saját céljaira is felhasználhatja. Ezáltal egy olyan „zombi PC”-vé válik a gépünk (tudtunk nélkül), mely spameket küld szét az Interneten vagy más számítógépek ellen indít támadásokat. Szakemberek szerint manapság akár 3-4 millió ilyen számítógép is jelen van a világhálón.

3.4. Védekezés a kórokozókkal szemben

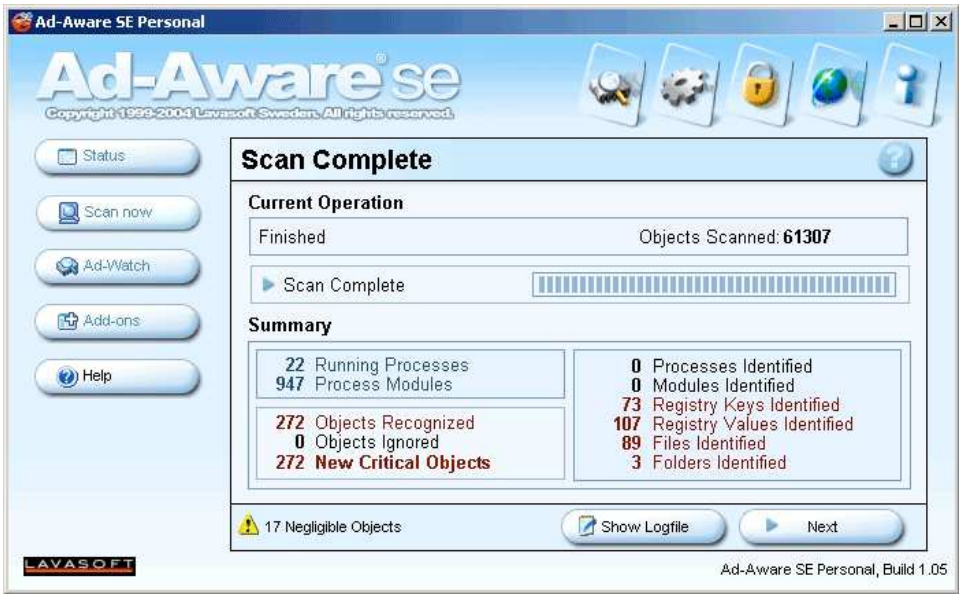
A védekezés legelterjedtebb módszere valamilyen vírusvédelmi szoftver alkalmazása. Ezek képesek felismerni a fertőzéseket és megoldást is kínálnak. Leginkább akkor hatásosak, ha rezidensen futnak a háttérben, valamint az Interneten keresztül le tudják tölteni a vírusdefiníciós adatbázis frissítéseit. Napjainkban már az is alapelvárás, hogy az Internetről letöltött tartalmakat és a levelezést is figyeljék.
Nézzük meg a NOD32 Antivirus System lehetőségeit. A több nagy díjat is bezsebelő szoftver jó példa arra, hogy mit kell tudni ma egy vírusirtónak. Kicsit puritán kinézetű, de roppant gyors. Természetesen memóriarezidens, már az operációs rendszer betöltődésétől kezdve véd minket. Tartalmaz fájlrendszer, dokumentum-, email és Internetes védelmet is. Képes frissíteni az adatbázisát Internetkapcsolaton keresztül, ha szükséges, akár naponta többször is. Naplózza a bekövetkezett eseményeket, így azok később bármikor visszanézhetők. Ki tudja szűrni a vírusokon kívül az Adware és a Spyware típusú fenyegetéseket is. Az automatikus figyelés mellett mi magunk manuálisan is indíthatunk keresést, melynek helyét tetszőlegesen megadhatjuk. Ez lehet cserélhető lemez, helyi lemez vagy akár hálózati meghajtó is. Fájlokat külön is ellenőriztethetünk vele, de bármely könyvtár is megadható és az alkönyvtáraiban is keres.

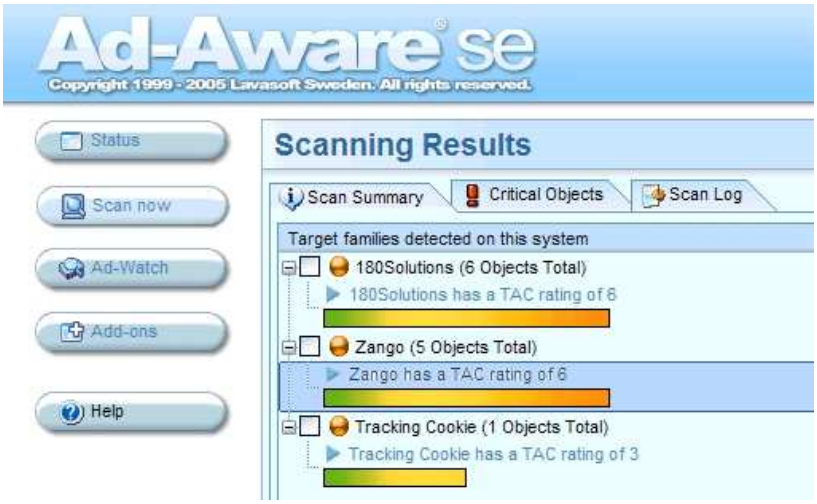


Vannak specializált programok is, melyek nem kifejezetten a vírusok elleni védelemre készültek, viszont nem árt néha lefuttatni őket. Ilyenek a reklám- és kémprogramok elleni szoftverek.

A reklámprogramok általában akkor települnek a gépünkre, ha kipróbálunk egy ingyenesen használható szoftvert. Az ingyenesség fejében viszont néha felugrik egy reklám vagy kapunk a programba egy reklámcsíkot. Vannak persze ennek agresszívabb változatai is, mint például amelyek a böngészőnk indulólapját megváltoztatják a reklámozandó weboldalra és egyszerű módon vissza sem tudjuk állítani a régi kedvencünket. Ilyenkor van szükség egy olyan megoldásra, mely segít a bajon.

Legismertebb képviselője az Ad-Aware SE Personal. Bár ez nem rezidensen fut, de elég bizonyos időközönként lefuttatni és gyanús objektumokat kerestetni vele. Reklámprogramokat, registry bejegyzéseket és gyanús cookie-kat képes kiszűrni, valamint képes azokat veszélyesség szerint besorolni, majd tetszés szerint eltávolítani. Adatbázisa frissíthető, így az újdonságokra is fel tudjuk készíteni.





A reklámprogramok mellett a kémprogramok is veszélyt jelentenek. Ezek megfigyelik a számítógép használóját, adatokat, email címeket, eltárolt jelszavakat gyűjtenek, majd ezeket elküldik Interneten keresztül a megfelelő embernek. Az előbb ismertetett Ad-Aware ezeket is felismeri és el tudja távolítani

3.5. Ártó szándékú emberek

Az ilyen emberek nagyban különböznek tudásbeli szintjükben. Vannak, akik csak ki akarják próbálni magukat és kevés kárt okoznak (például megváltoztatnak egy weboldalt). Vannak azonban komolyabb támadók is, akik sokszor szervezetten, csapatban hajtják végre akciójukat.

Támadások fajtái:

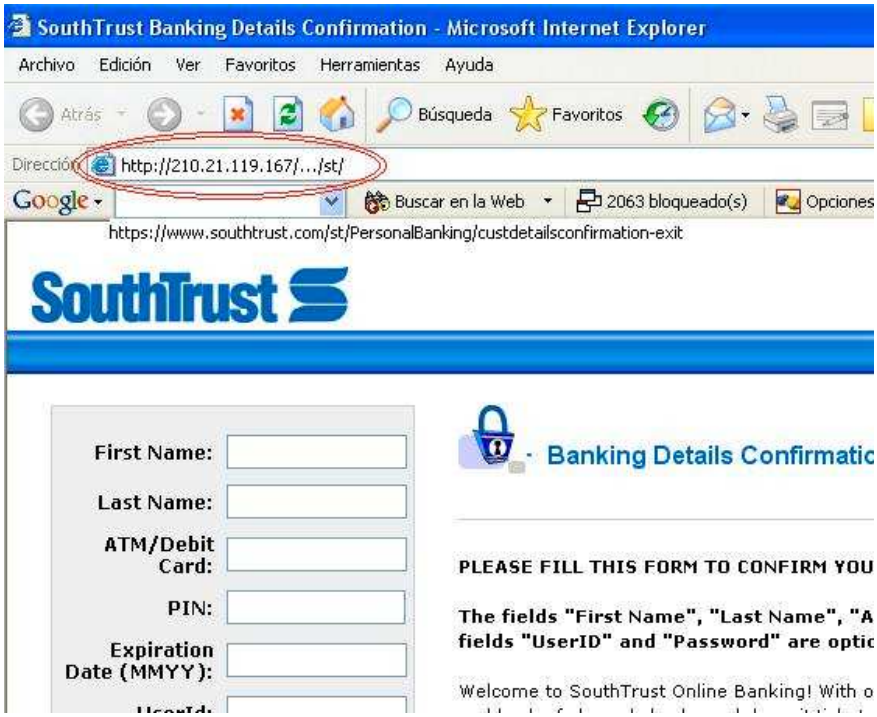
- Megszakítás – A rendszer vagy egy része használhatatlanná válik
- Elfogás – Egy jogosulatlan támadó hozzáférést szerez a rendszerhez, adatokhoz
- Módosítás – Egy jogosulatlan támadó hozzáfér a rendszerhez és adatokat módosít
- Gyártás – Egy jogosulatlan támadó hamis adatokat helyez el a rendszerben

Támadási mechanizmusok:

- Jelszó ellopása – cél a felhasználó jelszavának megszerzése
- Szociális technika – annak kihasználása, hogy a szociális kapcsolatban lévő emberek nem tartanak be minden szabályt egymásra nézve
- Hibák és kiskapuk – biztonsági rések kihasználása, tevékenység jogosulatlan indítása
- Hitelesítési hibák – hitelesítésre használt mechanizmusok átverése
- Protokoll hibák – protokollokban rejlő hibák kiaknázása
- Információ szivárgása – a támadó tudjon használni olyan szolgáltatásokat, melyekkel információ gyűjthető a hálózatról
- Szolgáltatás megtagadása – akadályozza a felhasználót a rendszer vagy egy szolgáltatás normális használatában; ezt legtöbbször egy túlterheléses támadással éri el

Talán külön is érdemes megemlíteni napjaink egyik gyakori és veszélyes támadási formáját, a phising-et, azaz az adathalászatot. Ennek az a lényege, hogy a csalók e-maileket küldenek szét nagyobb cégek, jellemzően bankok nevében. Ebben felhívják az ügyfél figyelmét, hogy különféle biztonsági okokból lépjen be felhasználói azonosítójával a rendszerbe. Csakhogy a mellékelt link nem a cég hivatalos honlapjára visz, hanem egy teljesen hasonló másolatra. Az ügyfél mit sem sejtve begépeli azonosítóját és jelszavát, mely azonnal a csalók kezére jut. Innentől kezdve pedig azt csinálnak, amit akarnak, akár leemelhetik a teljes összeget az ember számlájáról. Különösen veszélyes ez mostanság, mikor elterjedőben vannak az online banki

szolgáltatások. Ilyen támadás érte többször is a közelmúltban Magyarországon pl. a Raiffeisen bankot, de az egész világon milliós károkat okoz ez a tevékenység. A kivédésére szolgáló módszer a többszintű azonosítás. A tranzakciók végrehajtásához SMS-t küld a rendszer a felhasználó mobiltelefonjára egy meghatározott ideig érvényes megerősítő kóddal. A művelet csak ennek begépelésével véglegesítődik.



3.6. Védekezés tűzfallal

A tűzfalaknak teljesen más feladatuk van, mint a víruskeresőknek. Egyfajta elválasztást valósítanak meg a rendszerünk és a külső hálózat között. Figyelemmel kísérik a bejövő és a kimenő forgalmat is és ezeket ellenőrzik, szűrik, naplózzák. Lehet szó egy fizikai eszközről vagy egy programról is. Lényeges azonban, hogy a védelem mértékét mi alakítjuk ki azáltal, hogy egy szabályrendszert hozunk létre. Sajnos ezen szabályok tökéletes beállítása nem könnyű feladat, hiszen a hálózati kapcsolatot rengeteg porton keresztül rengeteg alkalmazás próbálja meg használni. A mi feladatunk kiválasztani, hogy ezek közül melyikekben bízunk meg és melyek tevékenységét állítjuk meg.

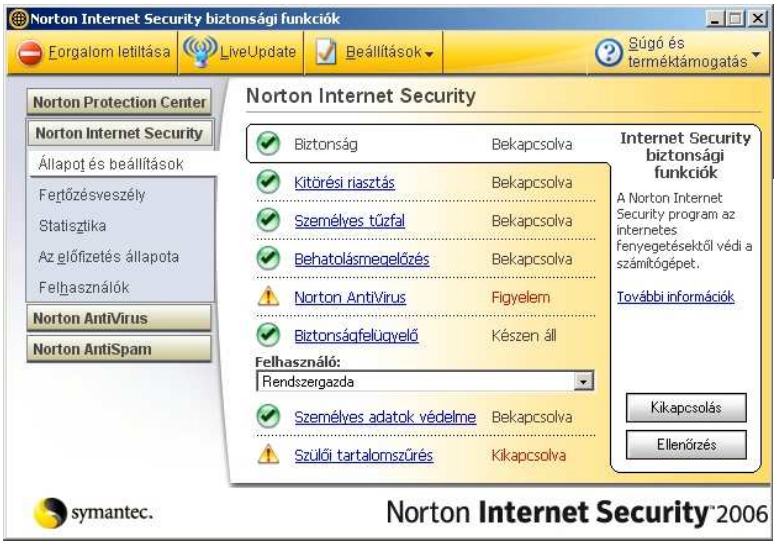
A tűzfalaktól elvárható funkciók:

- Csomagszűrés – Egy csomagot - forrásától függően - át kell engedni vagy el kell dobni. Előfordulhatnak nem szabványos csomagok is, ezek kiszűrésére is képesnek kell lennie.
- Portok figyelése – Figyelemmel kell kísérnie az összes használatban lévő portot, gyanús forgalom esetén tudnia kell blokkolni azt. Jó, ha ismeri az ún. port-scanning tevékenységet, amikor valaki távolról végigvizsgálja a nyitott portokat.
- Alkalmazások szabályozása – Az Internetet használó alkalmazások kimenő és bejövő adatforgalmát figyelnie kell.
- MD5 védelem – Az alkalmazásokról készül egy 128 bites digitális ujjlenyomat, mely egyértelműen beazonosítja őt. Ha megváltozik a program, az ujjlenyomat is vele változik. Ha ezt észreveszi, akkor kiszűrhető az a veszély, hogy az alkalmazást lecserélik egy hasonló, de ártalmas másolatra.
- Naplózás – Minden bekövetkezett esemény pontos nyilvántartása.
- Riasztás – Támadás, vagy bármilyen gyanús esemény bekövetkezésekor azonnal értesíteni kell a felhasználót
- Alapértelmezett szintek – Nem minden felhasználónak van olyan ismerete, hogy el tudja dönteni egy alkalmazásról, hogy megbízható vagy sem. Erre vannak a beépített biztonsági szintek, melyek a saját szabályozási rendet automatikusan használják.

Legismertebb változatai a Kerio Personal Firewall, a Sygate Personal Firewall, a Zone Alarm és a Norton Internet Security. Ezek mindegyike rendelkezik frissítési funkcióval, melynek használata erősen ajánlott, ha mindig naprakészek akarunk maradni.

Érdekesség, hogy Marcus J. Ranum, a tűzfalak atyja szerint 10 éven belül a hálózatbiztonsági szoftverek valamennyi típusa egyetlen hardverbe lesz integrálva, a piacot pedig az ezeket gyártó óriáscégek fogják uralni.

Egy-egy példa a mai szoftveres és fizikai megoldásokra:



És amit sokáig kevesen tudtak … maga a Windows rendszer is tartalmaz egy beépített tűzfalat. A szoftver a Windows XP-től kezdve került be az operációs rendszerbe. Alapvetően kikapcsolt állapotban van, ezért is nem tudta sok alapszintű felhasználó, hogy nem kell messzire menni egy kis védelemért. Sajnos elég szerény képességekkel rendelkezik, melyen valamelyest segít a Service Pack 2 telepítése. Azonban még így is csak a bejövő forgalom szűrésére alkalmas. A frissítés után már megengedi IP-cím és alhálózati maszk alapján kivételek definiálását.

Van egy érdekes előnye az összes többi tűzfallal szemben. Azok a rendszer teljes felállása után kezdik meg működésüket, mivel egy szolgáltatáshoz kötődnek. Ez azt jelenti, hogy egy bizonyos ideig (a szolgáltatás elindulásáig) a rendszer védtelenül áll. A Windows tűzfal viszont már aktív a rendszer betöltődésének megkezdésekor és egy nagyon szigorú szűrőt léptet életbe, melyet a teljes betöltődéskor cserél le a szokásos szabályrendszerre.

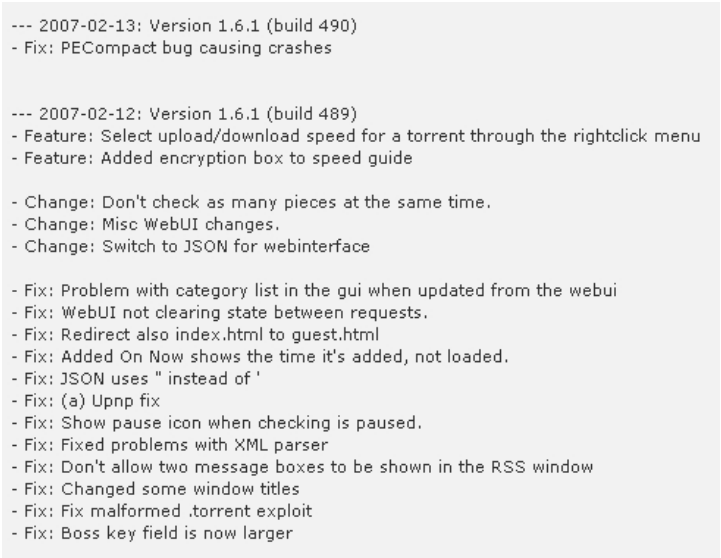
Ha a kockázatok ellenére is szeretnénk engedélyezni egy alkalmazás csatlakozását a hálózatra, lehetőség van kivételek létrehozására, ahol bármelyik programot vagy szolgáltatást manuálisan hozzáadhatjuk a megbízható listához. Továbbá azt is megtehetjük, hogy a kivételeknél egy általunk meghatározott portot nyitunk meg.

Az IPv4 mellett már az IPv6 protokollon keresztül érkező csomagok szűrésére is alkalmas.

3.7. Javítások

Hiba a legjobb vírusirtó, a legerősebb tűzfal, ha az alkalmazások vagy az operációs rendszer hiányosságai befoltozatlanul maradnak. Hiába blokkoljuk sikeresen az esetleges támadásokat, ha azok legközelebb ugyanúgy megtörténhetnek. Rengeteg felhasználó a világon úgy esik támadás áldozatául, hogy minimális erőfeszítéssel a bajt megelőzhette volna. Sajnos – a programozók jól tudják – nincs tökéletes program, mindig maradnak észrevétlen hibák a kódok megírása során. Ezek később kitudódva jó felületet adhatnak egy kis károkozásra. Ezt persze sokan tudják, most már külön csoportok foglalkoznak a hiányosságok felderítésével (jó és rossz csoportok egyaránt) és nyilvánosságra hozásával.

Ezekkel a problémákkal természetesen tisztában vannak maguk az alkalmazásokat fejlesztő cégek is és megtesznek mindent, hogy utólagosan helyrehozzák hibáikat. Egyik módja ennek, ha az alkalmazás következő generációját már úgy adják ki, hogy az addig észlelt hibák javításra kerültek. Ez azonban sokszor éveket vesz igénybe és legtöbbször a hiba olyan súlyos, hogy gyorsabb beavatkozásra van szükség. Erre találták ki az update vagy patch programokat, melyeket általában a cég hivatalos honlapján jelentet meg és onnan szabadon letölthető. Azon kívül, hogy kijavítanak bizonyos ismert hibákat, néha új funkciókkal is bővítik az alkalmazást. Ezeket mindig feltüntetik listaszerűen az egyes verzióknál. Tehát bizonyos időközönként mindenképp érdemes érdeklődni, hátha adtak ki frissítést valamelyik kedvenc alkalmazásunkhoz.



```
--- 2007-02-13: Version 1.6.1 (build 490)
- Fix: PECompact bug causing crashes


--- 2007-02-12: Version 1.6.1 (build 489)
- Feature: Select upload/download speed for a torrent through the rightclick menu
- Feature: Added encryption box to speed guide

- Change: Don't check as many pieces at the same time.
- Change: Misc WebUI changes.
- Change: Switch to JSON for webinterface

- Fix: Problem with category list in the gui when updated from the webui
- Fix: WebUI not clearing state between requests.
- Fix: Redirect also index.html to guest.html
- Fix: Added On Now shows the time it's added, not loaded.
- Fix: JSON uses " instead of '
- Fix: (a) Upnp fix
- Fix: Show pause icon when checking is paused.
- Fix: Fixed problems with XML parser
- Fix: Don't allow two message boxes to be shown in the RSS window
- Fix: Changed some window titles
- Fix: Fix malformed .torrent exploit
- Fix: Boss key field is now larger
```

Az operációs rendszerünk maga is egy program, ami szintén tartalmaz hibákat és ennél talán még fontosabb azok javítása. A Microsoft átlagosan havonta jelentet meg patch-eket „legfrissebb” operációs rendszereihez és alkalmazásaihoz (régebbi rendszerekhez csak korlátozott ideig ad ki frissítést, utána a támogatásuk megszűnik – pl. a Windows 98 és ME támogatása 2006 nyarán ért végleg véget). Ezek a havi csomagok több patch-t tartalmaznak a Windows rendszerhez és egyes alkalmazásokhoz (pl. Office vagy Internet Explorer). Néha nagyobb csomag, ún. service pack kerül kiadásra. Ez egy nagyobb horderejű frissítés, tartalmazza az addig kiadott összes javítást, bővítést és néha komolyabb változást is hoz az operációs rendszer életében (pl. Windows XP SP1 >> SP2). Technológiai előnyei is vannak egy-egy ilyen csomag feltelepítésének. A Windows XP SP1 annak idején az USB 2.0 és a Serial ATA szabványokat is beleépítette rendszerünkbe, így támogatva az újonnan megjelenő eszközöket és felgyorsítva a munkát velük. Mindezek elérhetők a Microsoft külön erre a célra fenntartott honlapján: http://windowsupdate.microsoft.com.

A védekezés az otthoni felhasználók mellett különösen fontos rendszergazdák esetén. Rájuk ugyanis nem csak egy rendszer, hanem sokszor egy egész intézmény számítógépes hálózata van bízva. Nekik már-már kötelező (lenne) figyelemmel kísérni a legújabb frissítések kiadását és ezek azonnali feltelepítését. Sajnos ezt sokan egyáltalán vagy csak későn teszik meg és ezzel nagy veszélynek teszik ki a kezükben lévő hálózatok biztonságát.

4. Az NTFS fájlrendszer

Az NTFS a New Technology File System rövidítése és a Windows NT 3.1-ben jelent meg először. Létrehozásánál több célt is szem előtt tartottak. Az adatvesztések minimalizálása érdekében biztosítani akarták a fájlrendszer kezeléséhez szükséges adatok állandó integritását, és a kényes adatokat óvni kellett az illetéktelen hozzáféréstől. Az egyre nagyobb kapacitású merevlemezek megjelenésével kezdett kevés lenni a FAT rendszerek által kezelt maximális fájlszám és kötetméret. Igény volt továbbá a drága hardveres redundancia-megoldások helyett szoftveres redundancia támogatására is.

4.1. Helyreállíthatóság

Alapkövetelmény, hogy az esetleges sikertelen műveletek vagy sérült fájlok helyreállíthatóak legyenek. Az NTFS bevezette az atomi tranzakció fogalmát, mely tranzakciók feldolgozása a „mindent vagy semmit” elvre épül. Ez az elv hasonló az adatbázisrendszerek világában megszokott elvvel, miszerint az atomi részekre bontott műveleteket egyenként hajtjuk végre, melyek ha egyszer elkezdődtek, be is kell fejeződniük. Ha ez a folyamat valahol megszakad, visszaáll az eredeti állapot. Ez megfelel az adatbázisos „rollback”-nek. Így biztosítódik a fájlrendszer konzisztenciája. Egy másik fontos tulajdonság, hogy az NTFS redundánsan tárolja a létfontosságú információkat, tehát ha megsérül egy szektor a lemezen, nem történik helyrehozhatatlan sérülés (mint pl. a FAT esetében elveszhet akár az egész kötet is!). Ez persze csak azt biztosítja, hogy a fájlrendszer elérhető marad, de arra továbbra sincs garancia, hogy minden egyes fájl örökké sérthetetlen lesz. Emellett az NTFS támogatja a RAID 1-et (adatok tükrözése) és a RAID 5-öt (adatok felírása csíkozva).

4.2. Hozzáférés

Biztosítani kell az illetéktelen hozzáféréstől való védelmet. Egy fájl egy biztonsági leíróval rendelkezik, mely a lemezen annak részeként van letárolva. Mielőtt egy folyamat megnyitna egy állományt, a Windows biztonsági alrendszere ellenőrzi, hogy van-e jogosultsága a művelet végrehajtásához.

4.3. Többszörös adatfolyamok (streamek)

Minden fájlhoz tartozó információ attribútumok formájában van implementálva (név, tulajdonos, tartalom, stb.). Minden attribútum egy stream, tehát egy fájlhoz több stream is tarozhat egyszerre, valamint könnyedén adhatunk új attribútumokat (streameket) egy fájlhoz. A mappák és fájlok tehát többszörös adatfolyamokat tartalmazhatnak. Ezeket a streameket akár külön-külön is írhatjuk vagy olvashatjuk. Minden fájlhoz tartozik egy alapértelmezett stream, mely „névtelen”. Az egyéb stream-ekre a nevükkel lehet hivatkozni kettősponttal elválasztva (pl. valami.doc : streamname). Ha megnézzük egy fájl tulajdonságait, az „Összegzés” fülön olyan információkat találhatunk, mint szerző, cím, stb. Ezek például a „Summary Information” nevű stream-ben tárolódnak.

4.4. UNICODE támogatás

Az Unicode 16 biten ábrázolja a karaktereket, így szinte minden földi nyelv ábécéje megjeleníthető. A mappák és fájlok nevei max. 255 karakter hosszúságúak lehetnek, valamint tartalmazhatnak UNICODE karaktereket, pontot és szóközt is.

4.5. Fájlok indexelése

Lehetőségünk van indexelési szolgáltatást igénybe venni, ezáltal felgyorsulnak a keresési folyamatok. Ez természetesen csak a szolgáltatás futása esetén használható ki. Nem csak NTFS rendszer esetén hatásos, de ott a leghatékonyabb a támogatás miatt.

4.6. Dinamikus bad-sector kezelés

Normál esetben egy hibás szektorból való olvasás esetén a folyamat megszakad és az adat elérhetetlenné válik. Ha hibatűrő NTFS-kötetünk van, akkor azonban a rendszer megpróbálja kinyerni az adatot, lefoglal egy másik szektort és berakja oda a megszerzett információt. Ezután megjelöli a hibás helyet. Ha nem lehetséges adatkinyerés, a megjelölés akkor is megtörténik.

4.7. Hard linkek, szimlinkek

A hard linkek segítségével többszörös elérési útvonalat hozhatunk létre egyazon fájlhoz vagy könyvtárhoz. Így különböző elérési útvonalakkal ugyanarra a fájlra vagy könyvtárra hivatkozhatunk. Meg kell jegyezni, hogy az eredeti fájlnak és a létrehozott linknek azonos köteten kell lennie. Ilyen linkeket mi is létrehozhatunk pl. az XP-ben az „fsutil hardlink creat” paranccsal. A másik fajta átirányítás a kapcsolódási pont vagy szimbólikus link (szimlink). Ennek szó szerint csak átirányítási feladatai vannak. Ha pl. van egy könyvtárunk C:\NewFolder néven és ez egy szimlink a C:\Windows könyvtárra, akkor a C:\NewFolder\win.ini fájl olvasásakor valójában a C:\Windows\win.ini fájlt érjük el.

4.8. Fájlok tömörítése

Az NTFS-ben beépített támogatás van az adattömörítésre. A szolgáltatás transzparens, ezáltal az alkalmazásokon semmilyen extra módosítást nem kell végrehajtani, hogy kezelni tudják a tömörített fájlokat. Ha mappákat tömörítünk, akkor az utólag bekerült fájlok is automatikusan tömörítetté válnak.

4.9. Naplózás

A naplóba minden olyan esemény bejegyzésre kerül, ami az adott köteten történt. Ez azért fontos, mert pl. a fentebb említett „rollback” művelet ezen naplófájl alapján tökéletesen végrehajtható.

4.10. Kvótakezelés

Az NTFS támogatja a felhasználói szintű kvótakezelést. Ez azt jelenti, hogy korlátozni lehet az egyes felhasználók lemezterület használatát. Ezen beállításra lehetőség van felhasználónként és csoportonként is. Ha valaki eléri a limitet, akkor egy „disk full error” hibaüzenettel értesíthető. A felhasználást folyamatosan naplózhatjuk és nyomon követhetjük az eseménynapló segítségével.

4.11. Linkkövetés

Fizikailag máshol elhelyezkedő fájlokhoz tudunk linket létrehozni parancsikonok segítségével. A háttérben fut az Elosztott Hivatkozáskövető Ügyfél (Distributed Link Tracking Client) nevű szolgáltatás, mely biztosítja, hogy ha a célfájlt átnevezzük vagy átmozgatjuk, akkor is működőképes legyen a link.

4.12. Titkosítás

Néha a komoly jogosultság-kezelés sem elég a fontos adatok védelmére. Ha mindenestül ellopják gépünket és megtekintik a merevlemezének tartalmát egy rendszergazda jogosultsággal, bármihez hozzáférhetnének. Ezért jött létre a Titkosító Fájlrendszer (Encrypting File System, EFS), mely a tömörítéshez hasonlóan transzparens az alkalmazások számára. A rendszer minden felhasználónak külön titkosítókulcsot ad, mely egyedi és megismételhetetlen. Ha egy fájlra vagy mappára ilyen titkosítást kérünk, akkor attól fogva ahhoz már csak az adott felhasználónak van hozzáférési joga. Sajnos ennek a rendszernek is van buktatója, mégpedig érdekes módon épp a túlzott biztonság. Ha valami okból pl. újra kell telepítenünk az operációs rendszert, természetesen az újonnan létrehozott felhasználók újra egyedi kulcsokat kapnak. Tehát a korábban letitkosított adataink lényegében örökre „titkosítva” is maradnak.

4.13. A fájlrendszer szerkezete

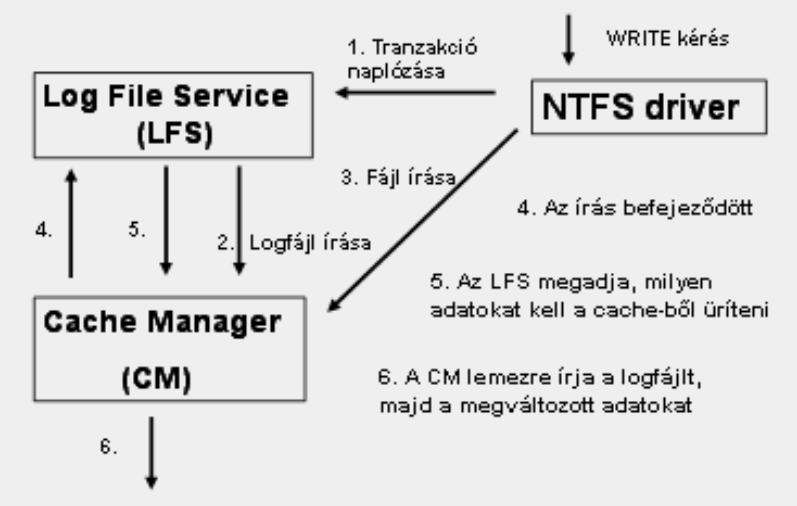
A fizikai lemez logikai partíciókra van osztva, ezek a kötetek. Egy lemezen akár több típusú kötet is helyet foglalhat. A clusterek az adattárolás alapegységei, egymás utáni szektorokból állnak. A rendszer csak a clustereket tartja nyilván, a szektorméretet nem, ezen függetlenség miatt tud nagy méretű lemezeket is kezelni. Meg kell még említeni az NTFS metadata információit (kötetleíró, boot információ, naplók), melyeket az alapelv szerint mind fájlban kell tárolni a lemezen.

4.14. Master File Table (MFT)

Ez az NTFS kötet „szíve”, lényegében fájlbejegyzések tömbje. A köteten található minden fájlról tartalmaz rekordot, még önmagáról is és pl. a metadata információkról is. Az első 16 bejegyzés foglalt az NTFS részére, ezek után következnek a felhasználói fájlok. Az egész MFT duplikálva van tárolva a lemezen, fizikailag távol egymástól, így hiba esetén sokkal nagyobb az esély arra, hogy a másik hely sértetlenül elérhető.

A metadata nevei mindig $-jellel kezdődnek, ezek alkotják az első bejegyzéseket. A legelején magára az MFT-re mutató mutatót találunk, utána pedig az MFT másolatára van hivatkozás. Egyéb fontosabb bejegyzések: $Logfile – az NTFS naplófájljára mutat, $Volume – információ az aktuális kötetről (neve, fájlrendszer verziószáma, dirty bit[2]), $AttrDef – a köteten támogatott attribútum-típusokat tárolja, \ – a gyökérkönyvtárnak van fenntartva, egy fájl megnyitásakor a keresés innen indul, $Boot – a boot-szektorra mutat, $BadClus – a hibás szektorok jegyzéke, $Secure – az egész kötetre vonatkozó biztonsági leírókat tartalmazza.

Ezeket ismerve, rendszerindításkor a következő folyamat zajlik le: $Boot fájl elérése, $MFT elérése és a memóriába töltése, $Logfile és egyéb metadata információk beolvasása, majd egy recovery művelet a fájlrendszer konzisztenciájának ellenőrzésére. Ezután már jöhetnek a fájltranzakciók, melyeket mindig megelőzi a gyökérkönyvtárhoz (' \ ') tartozó MFT bejegyzés megkeresése és memóriában való eltárolása. Egy lemezírási művelet így zajlik le:



4.15. A naplófájl felépítése

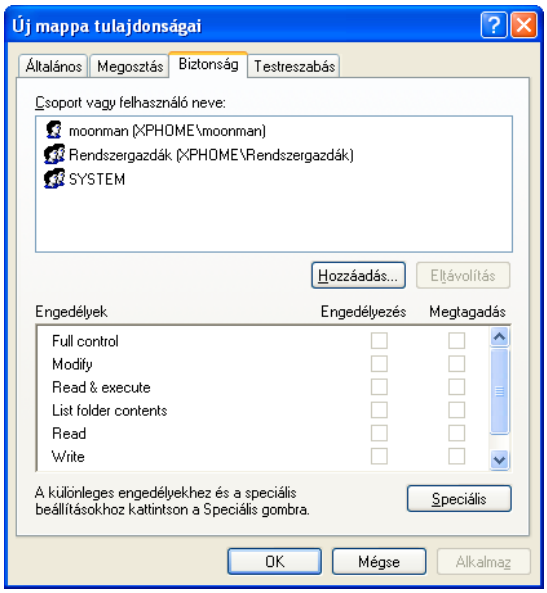
A naplót egy körkörösen íródó tömbként képzelhetjük el. Az első két bejegyzése fix: a fájlrendszer újraindításához szükséges információkat tartalmazza két példányban. Van

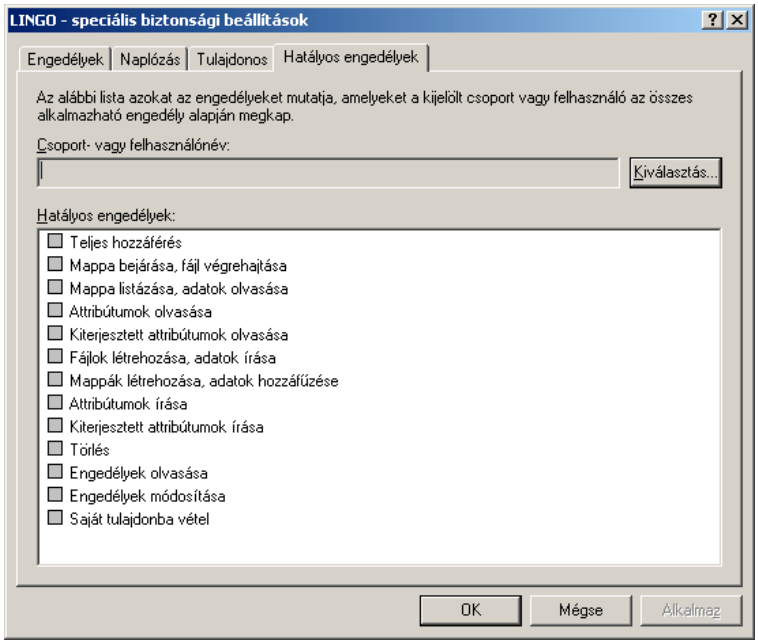
[2] A *dirty bit* az jelzi, hogy történt-e változás egy adott programlapon (azaz volt e olyan memória-írás, amely olyan címre hivatkozott, amely ezen a lapon van). Szerepe abban van, hogy ha egy lap kikerül a memóriából, akkor csak abban az esetben szükséges visszaírni a háttértárra, ha módosult, azaz dirty-bitje = 1.

egy redo infó, melyre akkor van szükség, ha egy tranzakció sikertelen volt. Ekkor mit és hogyan kell újra végrehajtani a sikeres befejezéshez. Van egy undo infó is, amely a sikertelen tranzakciók esetében leírja, hogy mit kell visszaállítani ahhoz, hogy az eredeti, változatlan állapotot kapjuk.

4.16. Hozzáférési jogosultságok

A különböző szintű felhasználók előre definiált sémák szerint kaphatnak jogokat. Ezeken felül lehetőség van speciális hozzáférés definiálására is, melyek pl. Windows XP esetén a következőképp néznek ki:



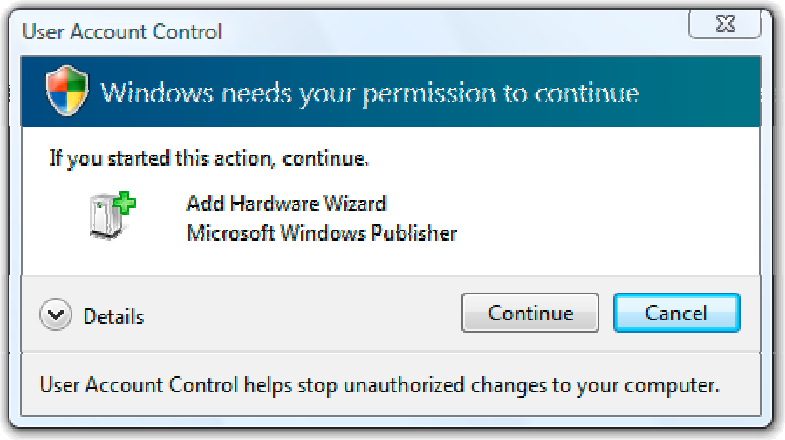


5. A Windows Vista biztonsági újdonságai

A Windows Vista 2007. januári megjelenésével a Microsoftnak sikerült létrehozni egy olyan operációs rendszert, mely – sok más között persze – biztonság terén messze felülmúlja elődeit. A Windows XP SP2 annak idején nagy előrelépést jelentett ugyan, de azóta a támadók módszerei is sokat fejlődtek. Eljött az idő a továbblépésre, egy megújult Windows kiadására. Bár a legszembetűnőbb változást inkább a felhasználói felületen vesszük észre, a háttérben is nagy változások mentek végbe. Adataink nagyobb biztonságban vannak, felügyeleti eszközök futnak észrevétlenül a háttérben, ezzel is segítve a megelőzést.

5.1. User Account Control (UAC)

Manapság nagyon sokan a felhasználói fiókjukat rendszergazdai jogosultsággal használják. Ez nagy kockázatot rejt magában, de sokszor elengedhetetlen, mert pl. a legtöbb alkalmazás a telepítéshez magasabb szintű jogosultságot követel meg. Erre találták ki az UAC-t, a felhasználói fiókfelügyeletet. A Vistában hiába vagyunk rendszergazda szintű felhasználók, alapból csak a „mezei” felhasználói jogokat kapjuk meg. Egy magasabb szintű joghoz kapcsolódó művelet végrehajtása előtt figyelmeztetést kapunk ennek szükségességére. Ekkor egy feladat erejéig rendszergazdák leszünk és a feladat a beleegyezésünkkel végrehajtódik. Ez óriási dolog biztonsági szempontból, de sajnos mindennek van hátulütője. Az újabb és újabb ilyen műveletek újabb és újabb ablakok felugrását eredményezik, melyeket mind érvényesítenünk kell. Ez sajnos a legtöbb felhasználónak egy idő után idegesítővé válhat. Az UAC egy másik fontos jellemzője, hogy a regisztrációs adatbázist és a fájlrendszer egyes területit virtualizálja. Ezzel megakadályozható a ténylegesen használt erőforrások károsodása, ugyanakkor az új megoldásból eredő kompatibilitási problémák is kiküszöbölhetővé váltak.



5.2. Mandatory Integrity Control (MIC)

Ez a technológia egy olyan infrastruktúrát valósít meg, melyben a felhasználók egy-egy integritási szinthez lesznek hozzárendelve. A rendszer minden objektum használata előtt ellenőrzi ezt a szintet. A felhasználókhoz vagy objektumokhoz rendelt szintazonosítók egy listában kerülnek tárolásra (System Access Control List - SACL). Ez hasonló a fájlrendszereknél ismert ACL listákhoz, de annál magasabb szintű, ugyanis a Vista először az SACL-t ellenőrzi és ha ott megtalálja a megfelelő biztonsági információkat, akkor tér át csak az ACL vizsgálatára. A MIC-nek 4 szintje van: alacsony, közepes, magas és rendszer. A rendszer szinthez tartoznak természetesen a rendszerfolyamatok, az alkalmazások pedig általában a közepes besorolást kapják. Érdekesség, hogy ez alól kivétel a beépített böngésző, ez ugyanis a legalacsonyabb integritási szintbe került. Mégpedig azért, hogy a csökkentett jogosultsági kör miatt kevesebb legyen egy esetleges fertőzés vagy károkozás veszélye.

5.3. Address Space Layout Randomization (ASLR)

Ezzel a Vista az illetéktelen hozzáférést akadályozza meg a rendszerfüggvényekhez. Hasonló már létezik egyes Linux / Unix disztribúciókban, de Windows rendszerekben ez az első megjelenése. A technológia hatékony védekezés a „return-to-libc” típusú támadások ellen, ahol a támadó rendszerfüggvényeket felhasználva próbálja elérni céljait.

5.4. Data Execution Prevention (DEP)

Ez a szolgáltatás már létezett Windows XP-ben is, de a Vistában alapértelmezetten fut és jobban konfigurálható. Célja a jogosulatlan kódfuttatások kiszűrése azáltal, hogy a memória egyes, adatszegmenshez tartozó területeit megjelöli és tiltja az innen való futtatást. Van hardveres és szoftveres formája is. A legújabb 64 bites Intel és AMD processzorok már tartalmaznak NX (No eXecute) biteket, melyeket az operációs rendszer fel tud használni a védelem kiaknázására.

5.5. PatchGuard

Érdekes technika, mely megakadályozza a kernel patchelését, azaz külső módosítását. Ez sajnos összeférhetetlen nagyon sok mai biztonsági szoftverrel. Ezek ugyanis alacsony szinten figyelték a kártevőket és azonnal be tudtak avatkozni, ha kellett. Sajnos azonban ezt a lehetőséget túl sok kártékony program tudta szintén kihasználni, így a Microsoft úgy döntött, megszünteti ezt a lehetőséget. Cserébe a Vista kínál pár új lehetőséget, mellyel a „jóindulatú” szoftverek figyelhetik az adatforgalmat, a fájlrendszert és a regisztrációs adatbázist.

5.6. Windows Service Hardening

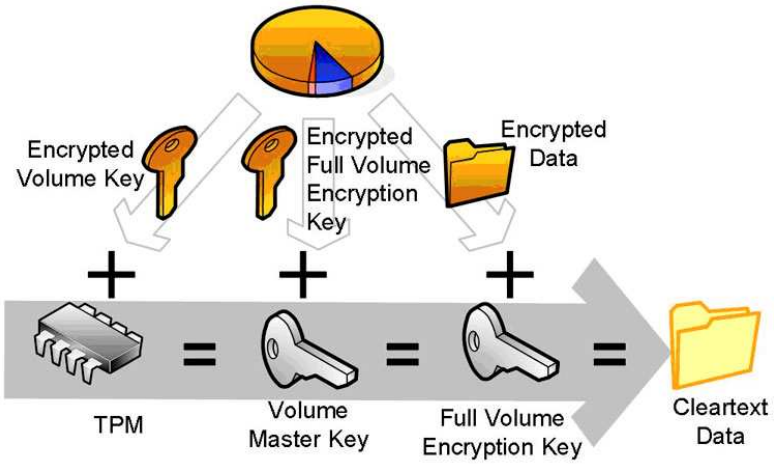
Mindezidáig a szolgáltatások a – teljes jogosultsággal rendelkező – Local System felhasználón keresztül futottak. Ezáltal egy szolgáltatás szinte bármit megtehetett, melyet természetesen a támadók ki is használtak. Ha ugyanis egy kártevő átvette felettük az irányítást, akkor „övé volt a rendszer”. Tipikus példája ennek a közelmúltban tevékenykedő Blaster féreg, mely az RPC (Remote Procedure Call) szolgáltatást támadta. A Vista a szolgáltatásokat a Local Service vagy a Network Service felhasználók alatt futtatja, melyek csak korlátozott jogokkal rendelkeznek.
A Vistában a processzekhez hasonlóan a szolgáltatások is kapnak azonosítót (SID), így könnyebben beazonosíthatók.

5.7. Network Access Protection (NAP)

A lényege, hogy csak azokat a számítógépeket engedi kapcsolódni a hálózathoz, melyek rendelkeznek a legújabb vírusfrissítésekkel és biztonsági javításokkal. Ha ez nem teljesül, csak a frissítések letöltésére van jogosultságuk, ezek telepítése után érhetik el újra a hálózatot.

5.8. BitLocker

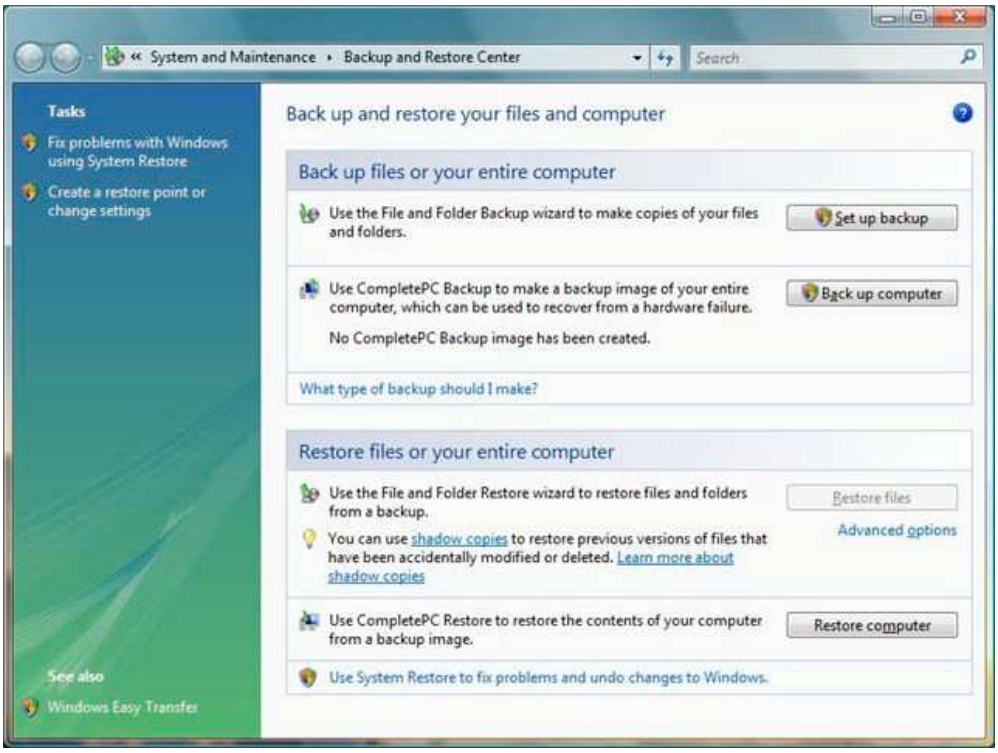
A technológia azoknak lehet hasznos, akik például könnyen elvesztik út közben laptopjukat, ugyanis ezzel a megoldással a merevlemez tartalma titkosítható, nem kerülhetnek rossz kézbe fontos adataink. Ha számítógépünk rendelkezik egy ún. TPM chippel, amely a titkosítási adatokat tárolja, akkor a biztonság még hatékonyabb. Egyébként lehetőség van a chippet egy USB meghajtóval is helyettesíteni. A technológiának olyan funkciója is van, hogy figyeli, hogy a rendszerbetöltések között módosultak-e fájlok, mert ez azt jelezheti, hogy valaki próbálja feltörni a védelmet.



5.9. Adatmentés

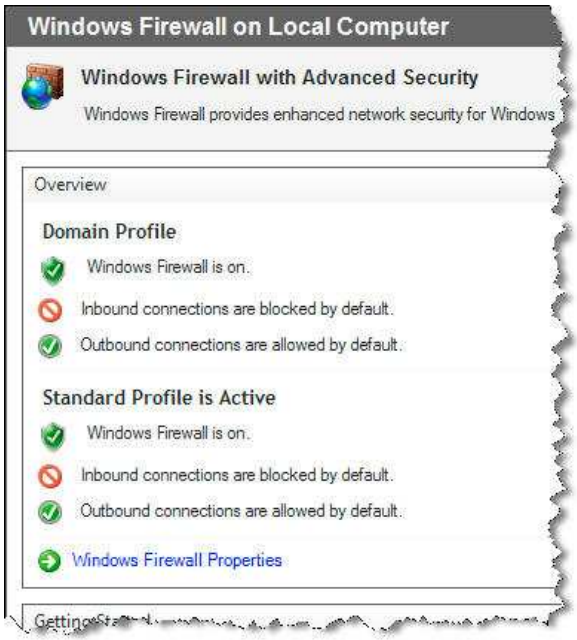
Ezen a téren a legfontosabb újdonság a teljes rendszermentés lehetősége. Hasonló a Norton Ghost képességeihez, a rendszerünket egy fájlba menthetjük, melyből később bármikor visszaállíthatjuk. Ez az image olyan formátumú, hogy akár Virtual PC segítségével virtuálisan megnyitható és módosítható is. Persze ha nem akarjuk az

egész rendszert lementeni, lehetőségünk van csak a fontosabb adatok archiválására, illetve későbbi visszaállítására.



5.10. Tűzfal

A Windows beépített tűzfala sokat fejlődött. Már az XP-ben is benne volt, de – mint tudjuk – csak a bejövő forgalmat szűrte, ezért ha a támadó valahogy már bejutott a rendszerbe, kifelé már azt csinált, amit akart. A Vista tűzfala a kimenő adatforgalmat is figyeli és csoportházirendeken keresztül állítható a felhasználók alkalmazásfuttatási joga.



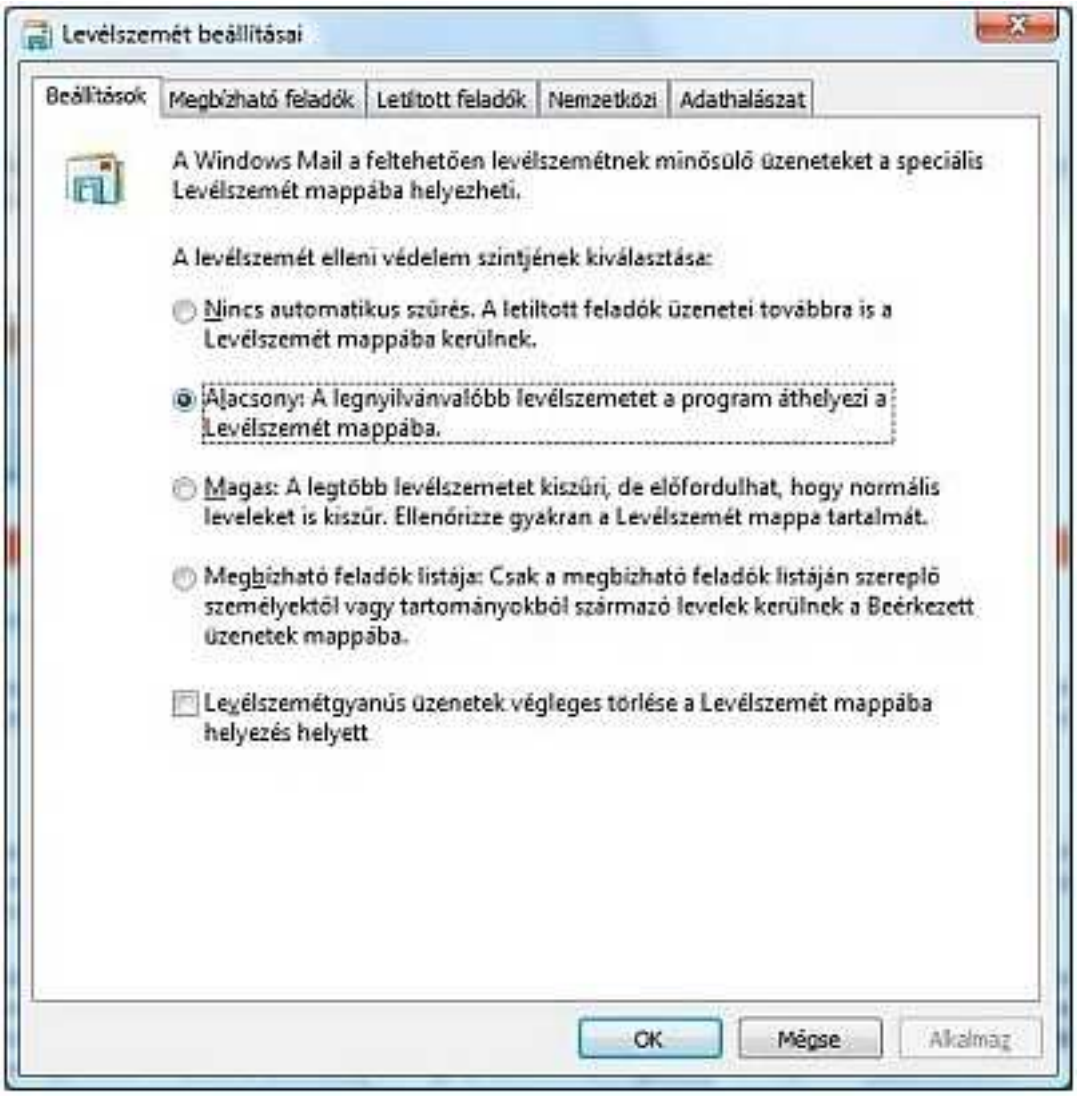
5.11. Böngésző

A Vista is tartalmaz beépített böngészőt, mégpedig az Internet Explorer 7-es változatát (pontosabban annak egy Vistás változatát, az IE7+-t), mely nagy átalakuláson ment keresztül. Kicsit elhaladt az idő a régi IE felett és megjelentek olyan alternatív böngészők, melyek egyre több szolgáltatást nyújtottak a felhasználóknak, ezért rohamosan csökkent az Explorer-t használók tábora. Ezért mostantól lehetőség van a közkedvelt többfüles böngészésre, de tartalmaz RSS szolgáltatásokat, felugró ablak blokkolót, stb. Mint már feljebb volt szó róla, a böngésző alacsony integritási szintre került, ami által sokkal kisebb a kártevők mozgástere. Az Explorer a háttérben egy külön mappát hoz létre, mely virtuálisan a merevlemeznek felel meg. A rendszerleíró adatbázisnak is létrejön egy árnyékmásolata, mely a böngészés végén törlődik. Így ebben a védett módban minimálisra csökken a károkozási lehetőség. Fejlődött az adathalászat elleni védelme is, sokkal jobb lett a szűrési funkciója. Ez a fajta támadás viszont olyan gyorsan fejlődik, hogy ez is csak korlátozott ideig fog teljes védelmet nyújtani (ennek is frissíthető az adatbázisa).

5.12. Levelezés

A Vistában lecserélték az eddig jól ismert Outlook Express-t a Windows Mail-re. Rengeteg új funkció került bele és biztonsági szempontból is sokat fejlődött, valamint a e-mailek tárolási technikája is változott, így gyorsabbá vált a használata. Az integrált Azonnali kereső a sok e-mailt tároló felhasználóknak nyújt igazi segítséget. Akár egy szó alapján is megtalálhatjuk a keresett üzenetet. Beépített spam-szűrőt tartalmaz, amelyet nem kell tanítani, automatikusan felismeri és elkülöníti a kéretlen leveleket. A szűrő érzékenysége igény szerint állítható. A Windows Mail az adathalászat ellen is védelmet nyújt, ugyanis észreveszi azokat a hivatkozásokat a levélben, melyek olyan

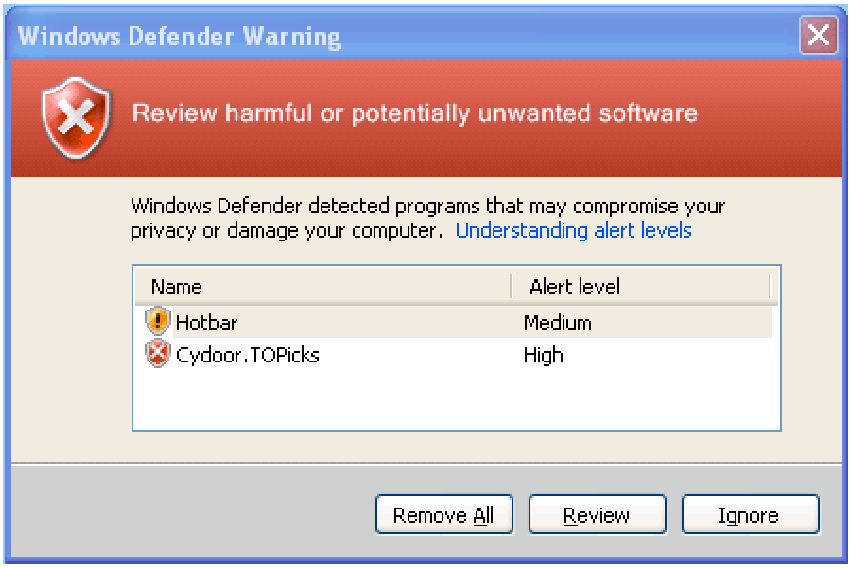
weboldalra visznek bennünket, ahol online csalás áldozatai lehetünk. Továbbá – természetesen – lehetőség van a programhoz tartozó definíciós fájlok időről-időre való online frissítésére, hogy mindig naprakészek maradjunk.



5.13. Windows Defender

Ez egy beépített alkalmazás, Microsoft-os fejlesztés, kártevők és kémprogramok ellen készült. A valós idejű védelem mellett a felhasználónak minimális beavatkozás szükséges egy esetleges rosszindulatú program eltávolításához. Figyeli az automatikusan induló és éppen futó alkalmazásokat, a hálózati adatokat. Adatbázisa folyamatosan frissül és működik az ismertebb védelmi szoftverekkel párhuzamosan is.

Sajnos a programot egyenlőre sok kritika éri, mivel már a jelenlegi spyware és adware programok között is rengeteg olyan van, amit a Defender nem képes kiszűrni és valószínűleg a jövőben csak nőni fog ez a szám. Ezért ha valaki egy korábbi Windows verzióban sikeresen használt ilyen malware-eltávolító szoftvereket, arra minden bizonnyal a Vistában is szüksége lesz … persze a Defenderrel kiegészítve.



6. Irodalomjegyzék

Andrew S. Tanenbaum – Számítógép-hálózatok

Béres Csaba Zoltán - Harka Győző : Számítógépes biztonság – Hálózati biztonság

Dravecz Tibor - Párkányi Balázs – Hogyan védjük hálózatba kötött számítógépes rendszereinket?

Dr. Leitold Ferenc – Számítógépes biztonsági kultúra

http://www.biztonsagportal.hu

http://www.microsoft.hu

http://www.msportal.hu

http://www.pcforum.hu

http://www.sg.hu

http://www.terminal.hu

http://www.symantec.com

http://hu.wikipedia.org