HADMÉRNÖK

IV. Évfolyam 4. szám - 2009. december

Sipos Marianna
sipos.marianna@zmne.hu

A WINDOWS ÚJ BIZTONSÁGI LEHETŐSÉGEI

Absztrakt

Az asztali gépes alkalmazások tömeges felhasználását felváltotta a szolgáltatás alapú architektúra, ahol az egyes szolgáltatások eléréséhez egyre gyakrabban használjuk az Internetet. A kívülről jövő támadások lehetősége és mennyisége ezzel megsokszorozódott. A Windows a .NET Framework szolgáltatásaival támogatja a védekezést a nem várt kártékony behatolások ellen.
A .NET Framework két biztonsági szolgáltatást kínál: A szerepalapú biztonság és a kóderedet-alapú biztonság lehetőségét. A szerepalapú biztonság a felhasználó jogosultságait ellenőrzi a .NET Framework Futtatókörnyezet által biztosított UAC segítségével, míg a kóderedet-alapú biztonság az assembly tanúsítványa segítségével olyan hozzáféréseket is korlátozhat amit az UAC nem tud.
Jóllehet a szolgáltatások használata a lehetőségek megismerését és némi kényelmetlenséget jelent, de biztonságunk érdekében a mindennapi életben is vállaljuk mindezt.

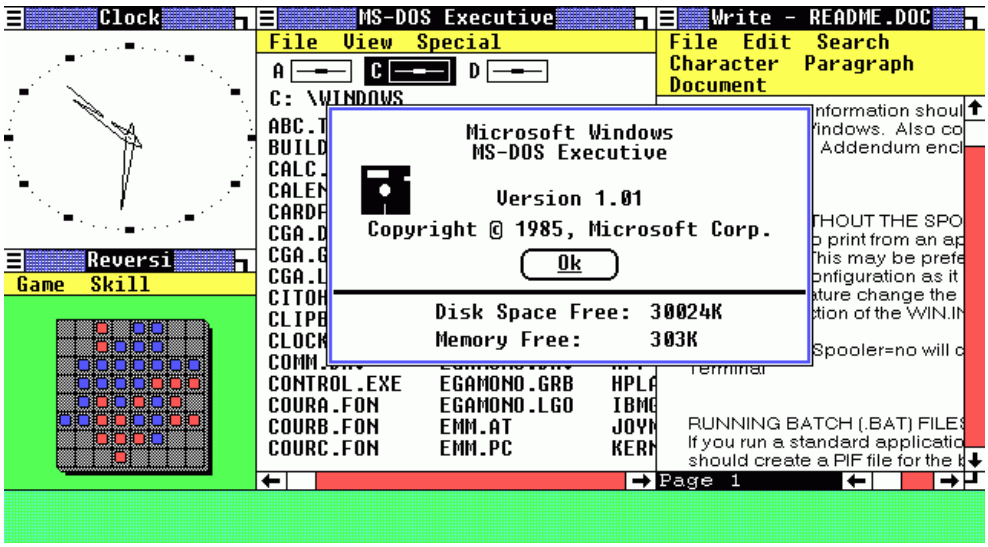
At first the masses used desktop applications, but the structure of applications is service oriented in these days. We use often the services through the Internet. The attacks coming from outside multiplied. The services of .NET Framework give the potentiality protection against malicious attacks.
.NET Framework has two kinds of security services: Role-based security and code access security. The role-based security controls the users permissions with the User Account Control service. The code access security controls the assemblies permissions used the assemblies certificate. CAS gives us the chance to protect our computer from malwares.
The use of security services is comfortless, and needs some preparedness, but the situation is the same in casual.

Kulcsszavak: *szoftver, biztonság, Windows ~ software, security, Windows*

Előzmények

A PC-k tömeges elterjedése növelte az igényt, hogy a számítógépeket ne csak egyedi programok írására, hanem a mindennapi élet feladatainak megkönnyítésére szolgáló

alkalmazások futtatására is használjuk. A Windows létrehozásakor a Microsoft célja az volt, hogy asztali gépekre készülő alkalmazások futtatását tegyék lehetővé mindenkinek, elérhető áron. A kényelmesen kezelhető grafikus felület (1. ábra) egyszerűvé tette a monitoron a tájékozódást, az egér használatával gyorsan és egyszerűen lehetett a programokat indítani, kezelni.



1. ábra A Windows 1.0 grafikus felülete [1]

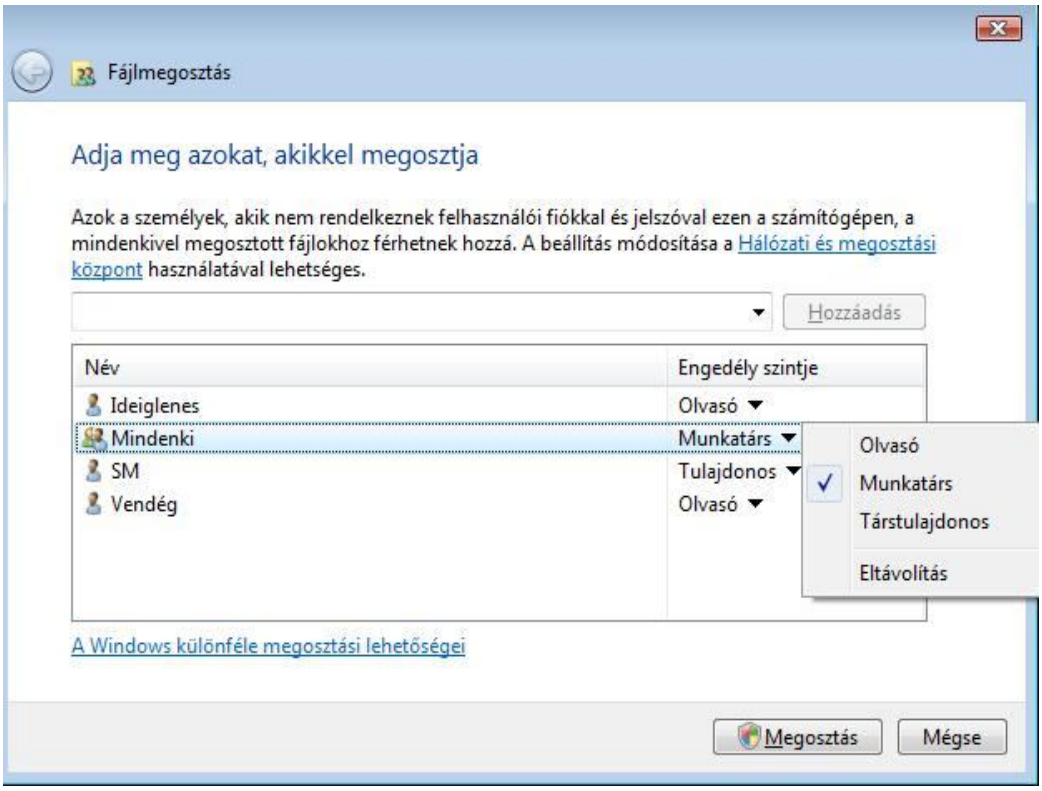
Megbízhatóságát üzleti alapon épp annyira biztosították, hogy a tömeges felhasználás során az átlagos felhasználó ne ütközzön problémákba. A cég üzleti sikerei annak köszönhetőek, hogy piackutatással meghatározták az igényeket és pontosan azokhoz illesztették a szoftver képességeit. Sem többet, sem kevesebbet nem adott az elvárásoknál. Ha nem felel meg a felhasználói igényeknek, nem terjed el a piacon, másrészt viszont a vártnál minél többet nyújt, annál jobban csökken az üzleti haszon.

Akkoriban főként egyedi gépeken futó alkalmazások felhasználására volt igény. Egy gépet többnyire egy személy használt, vagy egy család, esetleg egy kis munkahelyi közösség. Mivel nem volt internethozzáférés, nem kerültek a gépekre a szülők elől titkolt magánbeszélgetések, vagy munkaidőben végzett magánügyek adatai, és persze mások sem férhettek hozzá a család vagy a munka adataihoz, amivel aztán visszaélhettek volna. Ami a gépen volt, azt a felhasználók mindannyian tudták. Az asztali gépeknél ma is ritkán van szükség a közös használatból eredő mappahozzáférés védelmére. Hálózati kapcsolatok nélkül az idegen felhasználó legfeljebb az egyedül hagyott gép elé ülve juthatott adatokhoz. Ennek védelmét egy egyszerű jelszó bekérésével megoldhattuk. A legtöbb felhasználó ezzel az eszközzel sem élt.

Hálózat és internet használat

A hálózatok használatának és az internet elérésének elterjedése megváltoztatta a számítógépek használatát. Ma már az a ritka, ha offline használjuk gépeinket. Általában a bekapcsolás során bejelentkezünk a hálózatra. A szoftvereket is jó ideje úgy fejlesztik, hogy működésükhöz szerverekkel kell kommunikálniuk.

Az első megoldás adataink védelmére, vagy megosztására nézőpont kérdése, a nyilvános mappa és a mappák megosztásának lehetősége volt. Itt még speciális beállítások is rendelkezésünkre álltak, megadhattuk, hogy az adott könyvtárat mely felhasználói csoport és milyen engedéllyel érheti el. (2. ábra)

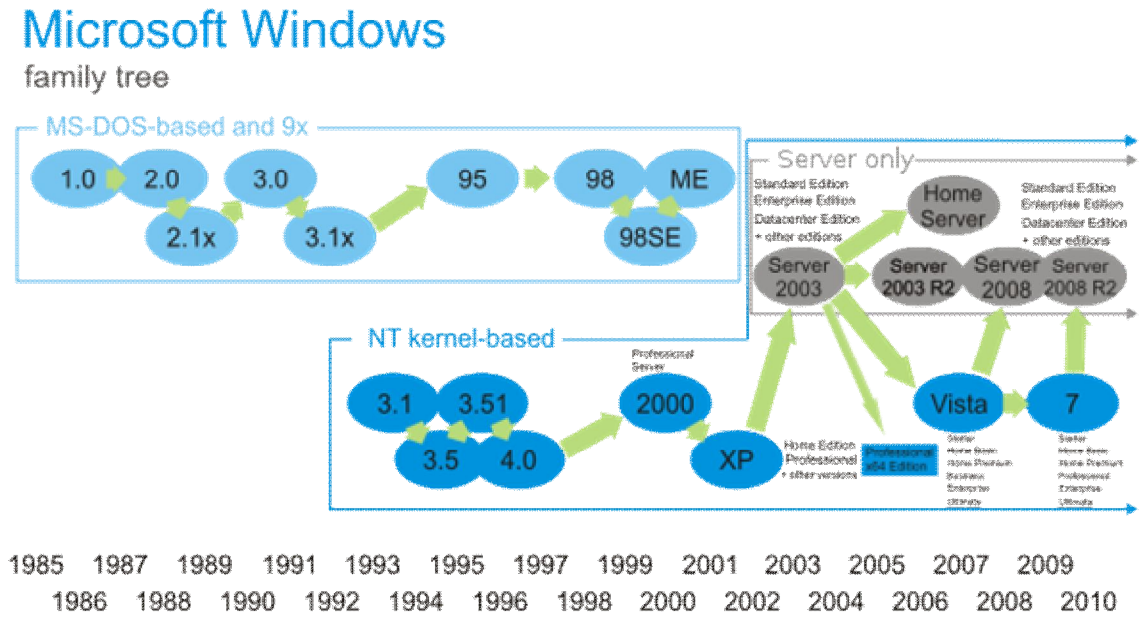


2. ábra A mappák megosztását beállító ablak

Lehetőség volt a felhasználói jogok korlátozására. Ezzel a rendszergazdák többnyire a rendszer működőképességének megőrzése érdekében éltek oly módon, hogy bizonyos mappák módosítását megtiltották. Nagyon ritkán használták az egyénre szabás lehetőségét. Általában megelégedtek az alapértelmezésben létező rendszergazda és általános felhasználó csoportok használatával. Beállították az általános felhasználók jogosultságait és akinek több hozzáférésre volt szüksége, az átkerült a rendszergazda csoportba. Tehát a szűk lehetőségeket szűkösen használták.

A hálózatok használatának egyre sokoldalúbbá válása és a kívülről érkező egyre kifinomultabb támadások további védekezési lehetőségeket igényeltek. A .NET Framework, mely Windows XP esetén még egy opcionálisan telepíthető réteg az operációs rendszer felett, a Vista megjelenésével beépült az operációs rendszerbe.

Ha megnézzük a Windows fejlődését bemutató ábrát (3. ábra), két nagy változást láthatunk benne. Az első, amikor a grafikus felület az operációs rendszer részévé vált egybe esett a 16 bitről 32 bitre történő váltással. A második a .NET framework beépülése az operációs rendszerbe egyben a 32 bitről 64 bitre váltás megvalósítása. Ha már az első esetben kiemeltük a grafikát megjegyezném ezen a területen is jelentős a válttozás. Míg a korábbi Windows-ok a bitképes ábrákat támogatták a WPF (.NET 2.0) megjelenésével áttér a vektorgrafikus képábrázolásra.



3. ábra A Windows fejlődése [2]

Természetesen sok további változást is hozott a .NET bevezetése, ezek közül ebben a cikkben a biztonsági szolgáltatásaival foglalkozunk.

.Net hozzáférés-szabályozás

Hozzáférés-szabályozás alatt a hálózaton vagy a számítógépen található objektumok elérésének engedélyezését értjük felhasználók, csoportok vagy számítógépek részére. A szabályozás elemei:

- Engedélyek
- Objektumok tulajdonjoga
- Engedélyek öröklődése
- Felhasználói jogok
- Objektumok naplózása

A szabályozható objektumok a következők:

- Fájlok, mappák
- Active Directory objektumok
- Beállításjegyzék objektumok (registry)
- Rendszerobjektumok (pl. folyamatok, feladatütemező, nyomtatásvezérlés, naplózás)

Az objektumok típusa határozza meg, milyen engedély adható. Pl. az NTFS-engedélyek és hozzáférési korlátozásaik a következő táblázatban olvashatók:

Speciális engedélyek	Teljes hozzáfér	Módosít	Olvas és végrehajt	Mappa tartalomlista	Olvasás	Írás
Mappa bejárása, fájl végrehajtása	x	x	x	x		
Mappa lista, adat olvasása	x	x	x	x	x	
Attribútum olvasása	x	x	x	x	x	
Kiterj. Attribútum olvasása	x	x	x	x	x	
Fájl létrehozás, írás	x	x				x
Mappa létrehozás, adat hozzáfűz	x	x				x
Attribútum írása	x	x				x
Kiterj. Attribútum. írása	x	x				x
Almappák és fájlok törlése	x					
Törlés	x	x				
Engedély olvasása	x	x	x	x	x	x
Engedély módosítása	x					
Saját tulajdonba vétel	x					
Szinkronizálás	x	x	x	x	x	x

Felhasználói fiókok felügyelete

A felügyeletet az UAC (User Account Control) végzi. Feladata, hogy segít megelőzni a számítógépen végzett nem engedélyezett változtatásokat. A változtatások előtt az UAC előbb engedélyt kér. Ha van az adott felhasználónak jogosultsága, az engedélyt megkapja. Ha nincs jogosultsága, rendszergazdai jelszót kér. Ez a megoldás teszi lehetővé, hogy ha egy rendszergazdai jogokkal rendelkező felhasználó nem rendszergazdaként lép be, akkor is el tudja végezni a munkája során adódó rendszergazdai jogosultságot igénylő feladatokat, és az aktuális user nevében nem lehet a gépre a háttérben rosszindulatú szoftvereket (malware) kémprogramokat telepíteni.

Az UAC üzenetei:

- **A Windows a beleegyezését kéri a folytatáshoz**
  Amikor olyan Windows programot futtatunk, mely hatással van más felhasználók adataira.

- **Egy programnak engedélyre van szüksége a továbblépéshez**
  Ha a futtatni kívánt program rendelkezik digitális aláírással, mely tartalmazza a nevét és a kiadó nevét. Eldönthetjük megbízunk-e benne.

- **Egy azonosítatlan program kér hozzáférést a számítógéphez**
  Ha a futtatni kívánt program nem rendelkezik digitális aláírással, nem azonosítható. Döntsük el, hogy megbízunk-e benne.

- **Ez a program le van tiltva**
  A rendszergazda által letiltott program. Ha szüksége van rá, kérjen engedélyt a futtatáshoz.

Kóderedet-alapú biztonság

A CAS (Code Access Security) [3] az alkalmazás jogosultságát nézi, nem a felhasználóét. Ehhez eszközként a tanúsítvány ellenőrzést használja. A CAS segítségével a szerepalapú biztonsággal nem korlátozható hozzáférések is ellenőrizhetők. pl.

- Az adott alkalmazás tud vagy nem tud Web kérést küldeni az internetre.
- Egy alkalmazás kérhet vagy nem DNS-t

Amint azt a 4. ábrán is láthatjuk 7 alapértelmezett engedélyhalmaz áll rendelkezésünkre:

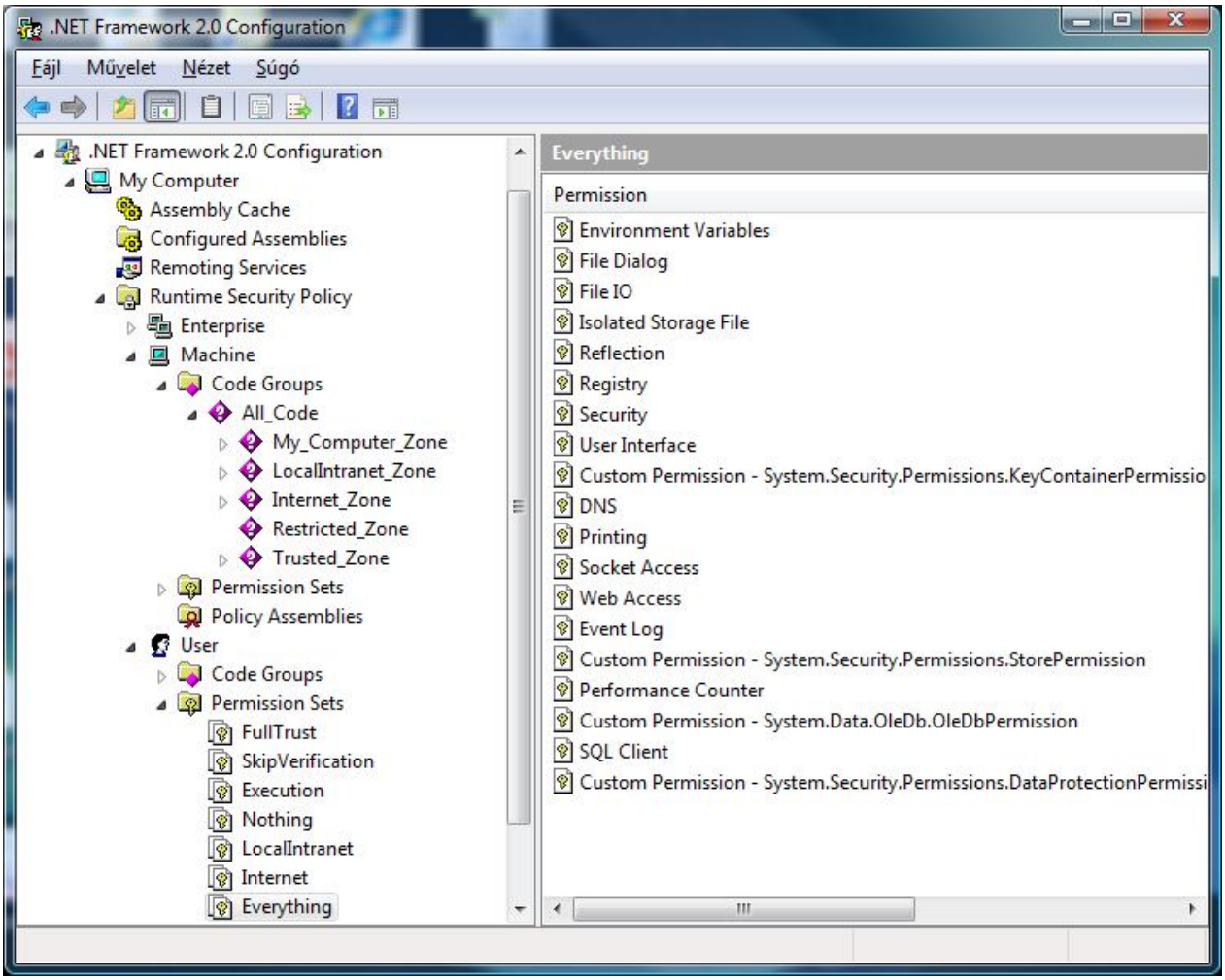
- FullTrust: Nem ellenőrzi a CAS
- SkipVerification: Elkerülheti az ellenőrzést. Javítja a teljesítményt, feláldozza a biztonságot.
- Execution: Csak futhat.
- Nothing: Még csak nem is futhat.
- LocalIntranet
- Internet
- Everything: Összes standard, beépített engedély. Abban különbözik a FullTrust-tól, hogy a CAS ellenőrzés végrehajtódik rajta.

A .NET Framework Configuration (4. ábra) eszköz segítségével [4] mi magunk is létrehozhatunk engedélyhalmazokat, és meghatározhatjuk a hozzájuk tartozó engedélyeket.

A biztonsági házirend három házirend szintet bocsát rendelkezésünkre. Ezek:
- Enterprise
- Machine
- User

A házirendek mindegyikéhez tartoznak kódcsoportok. Az assemblyket kódcsoportokba sorolhatjuk. Az egyes kódcsoportokhoz kiválaszthatjuk az engedélyhalmazt, melynek engedélyeivel rendelkezik. Alapértelmezésben az adott gép (machine) házirendje tartalmaz az All_Code csoporton belül kódcsoportokat. Ezek mindegyike zóna. Vagyis egy kód attól függően tartozik a csoportba, hogy honnét futtatjuk. A következő zónák állnak rendelkezésünkre (4. ábra):

- My_Computer_Zone
- LocalIntranet_Zone
- Internet Zone
- Restricted_Zone
- Trusted_Zone



4. ábra Kódcsoportok és engedélyhalmazok

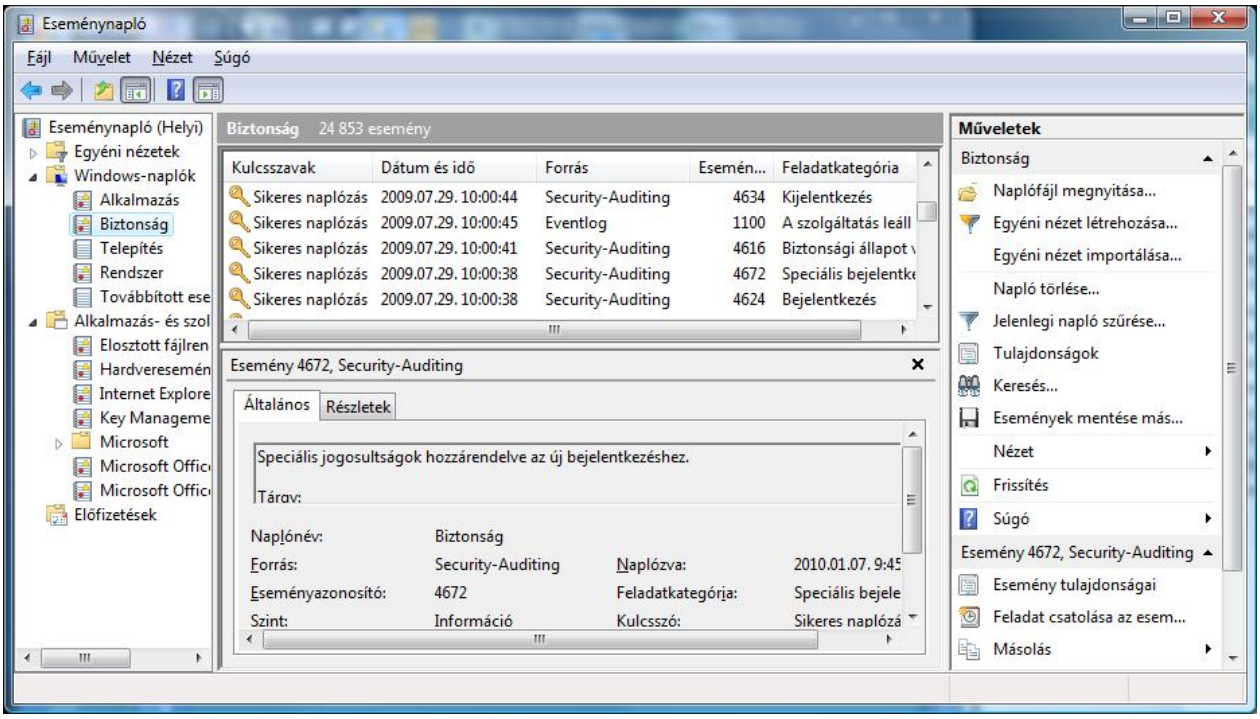
További kódcsoportokat mi magunk hozhatunk létre.

A futtatott kódnál a házirend kiértékeli mindhárom házirend szintet. Besorolja a kódot az ott megadott kódcsoportok valamelyikébe, majd meghatározza az engedélyhalmazt, és az abban megadott engedélyeket. A három házirend által meghatározott minimális engedély áll rendelkezésre a kód futásához.

Ha már meghatároztuk az egyes kódok lehetőségeit, a hibás esetek elemzéséhez még a naplózást kell beállítanunk.

Naplózás

A naplózás beállítására a vezérlőpult, felügyeleti eszközök, eseménynapló (5. ábra) szolgáltatás ad lehetőséget.



5. ábra A Vista Eseménynaplója

Összegzés

A szinte mindent megengedő Windows egy alapos, de bonyolult biztonsági rendszert dolgozott ki a .NET Framework szolgáltatásaként. Két lehetőség volt a bevezetésnél. Vagy alapértelmezésben nem szorítja rá a felhasználót a biztonsági szolgáltatásokra, és akkor a felhasználó nem is vesz azokról tudomást. Vagy a gépen futtatott kódok engedélyt kérnek a biztonságot veszélyeztető helyek hozzáféréséhez.

A .NET futtatókörnyezet szolgáltatásai „sokkolták” a felhasználók nagy részét. A számos bírálat ellenére, talán túl gyorsan érkezett? Vagy a felhasználói tömegek nem igénylik? Vagy amit soha be nem vallanánk, az ablakok olyan figyelmeztetéseket küldenek, melyeket nem értünk, így fölöslegesnek ítélünk?

Gondoljunk arra, ha egy biztonságos környéken élve nem zárjuk a lakásokat, mert fölösleges gond kulccsal a zsebünkbe közlekedni. Aztán egyre több turista jön a nagyvilágból és viszik hírét ennek a nyugalmas környéknek, ahol még az ajtót sem kell bezárni. Meghallják ezt a besurranó tolvajok is. S a könnyű rablás reményében megszállják a környéket. Rögtön megváltoznak a szokásaink és elkezdjük zárni az ajtókat, garázsokat, kertkapukat, majd megerősítjük ablakainkat, riasztót szerelünk a lakásra. Természetesen a munkahelyünk ugyanezt teszi. Pedig milyen kényelmetlen sok kulcsot cipelni a zsebünkbe, azonosító kártyákra figyelni, riasztó kódokat, jelszavakat megjegyezni!

Hivatkozások:

[1] A kép forrása: Wikipedia, http://en.wikipedia.org/ History of Microsoft Windows http://upload.wikimedia.org/wikipedia/en/4/4e/Windows1.0.png

[2] A kép forrása: Wikipedia, http://en.wikipedia.org/ Timeline of Microsoft Windows http://en.wikipedia.org/wiki/Timeline_of_Microsoft_Windows

[3] Albert I., Balássy Gy., Charaf H., Erdélyi T., Horváth Á., Levendovszky T., Péteri Sz., Rajacsics T.: A .net framework és programozása, szak kiadó, 2004.

[4] .NET Framework 2.0 Configuration tool súgója.