DIPLOMAMUNKA

Marozsán Gergely

Debrecen
2009

Debreceni Egyetem, Informatikai Kar,
Információ Technológia Tanszék

Számítógépes biztonság MS platformon

Témavezető:
Dr. Krausz Tamás
egyetemi adjunktus

Készítette:
Marozsán Gergely
programtervező
matematikus
hallgató

Debrecen, 2009

Tartalomjegyzék

Bevezetés

A biztonság az egyik legfőbb beszédtéma az IT szakemberek körében. A mai felméréseket tekintve abban a 4-esben szerepel, ami a legtöbb fejtörést okozza, és ez nem csoda. Hiszen az elmúlt néhány évet tekintve jelentős biztonsági fenyegetést élt át bárki, aki számítógépet használt, főleg Microsoft Windows operációs rendszerrel.
Akár vírusos támadás, trójai faló, féreg-támadás, vagy csak egy rosszindulatú kód a számítógépen vagy a szerveren, jelszó ellopás van a háttérben, mindenki veszélyben van. Egy dolog azonban biztos: azok, akik nem tesznek semmit a biztonságuk érdekében, nagyon könnyen sebezhetővé válhatnak, és mindenüket elveszíthetik.
Ami pedig ennél is rosszabb, hogy a hackerek mindent megtesznek azért, hogy információkat szerezzenek meg a szervezetekről, rólunk, legyen az akár egy jelszó vagy hitelkártyaszám.
A vállalatok és mi, hétköznapi emberek pedig kénytelenek vagyunk mindent megtenni azért, hogy ezt elkerüljük.
Azok a szervezetek és magánszemélyek pedig, akik a Microsoft termékeit használják, a leginkább azok, akik veszélyben vannak. Mivel a Microsoft a világ első számú beszállítója, ezzel az első számú célpontja is egyben.
A biztonság lényege az információ megvédése. Mit tehetünk, tehetnénk fel a kérdést.

- azonosítsuk a személyeket, amikor belépnek a hálózatba
- állapítsuk meg megfelelő szinteket az emberekhez, és adjunk nekik szintekhez megfelelő hozzáféréseket
- bizonyosodjunk meg arról, hogy ha valaki módosít egy adatot, akkor ő az a személy, akinek joga van azt módosítani
- garantáljuk az információ bizalmasságát, miután elhelyeztük a hálózatban
- garantáljuk az információ elérhetőségét, miután elhelyeztük a hálózatban
- bizonyosodjunk meg az adatok integritásáról
- ellenőrizzük a hálózaton belüli tevékenységeket
- ha fontos adminisztratív tevékenységeket folytatunk, bizonyosodjunk meg róla, hogy hálózatunk biztonságos minden időben

Mindezekre a tevékenységekre, különböző kölcsönhatási területek vannak:

- **Local**, helyi kölcsönhatási terület, az emberek helyi szinten kerülnek kapcsolatba a rendszerrel, védett területek, akár csatlakoznak akár nem egy hálózathoz.

- **Intranet**, távoli kapcsolatban állnak a rendszerrel a személyek, ezek szintén védettek kell hogy legyenek, akár a LAN-on (Local Area Network), akár a WAN-on (Wide Area Network) találhatóak
- **Internet**, azok a rendszerek, amelyek nyilvánosnak látszanak, szintén védettek kell hogy legyenek minden típusú támadástól, ezek vannak a legrosszabb helyzetben, mivel a bizalmas hálózat határain kívül vannak
- **Extranet,** ezek is bizalmas hálózatnak látszanak, de ki vannak téve ügyfeleknek, partnereknek, és más klienseknek. A legnagyobb különbség az Internet és Extranet rendszerek között, hogy míg az Internet rendszerben lehet authentikáció (hitelesítés), addig az Extranet rendszerben mindez kötelező.

Bármi is legyen a terület, a biztonság egy tevékenység, ami 3 dolgon alapszik:
Emberek, számítógépek, és folyamatok.

- **Emberek**, ők a végrehajtói a folyamatoknak, és egyben a fő használók.
- **Számítógépek**, képviselik és ábrázolják a technológiát, rengeteg eszközzel támogatják a biztonsági folyamatokat.
- **Folyamatok**, melyek azért jöttek létre, hogy eljárások és szabványok legyenek a biztonság érdekében.

CDS- Castle Defense System

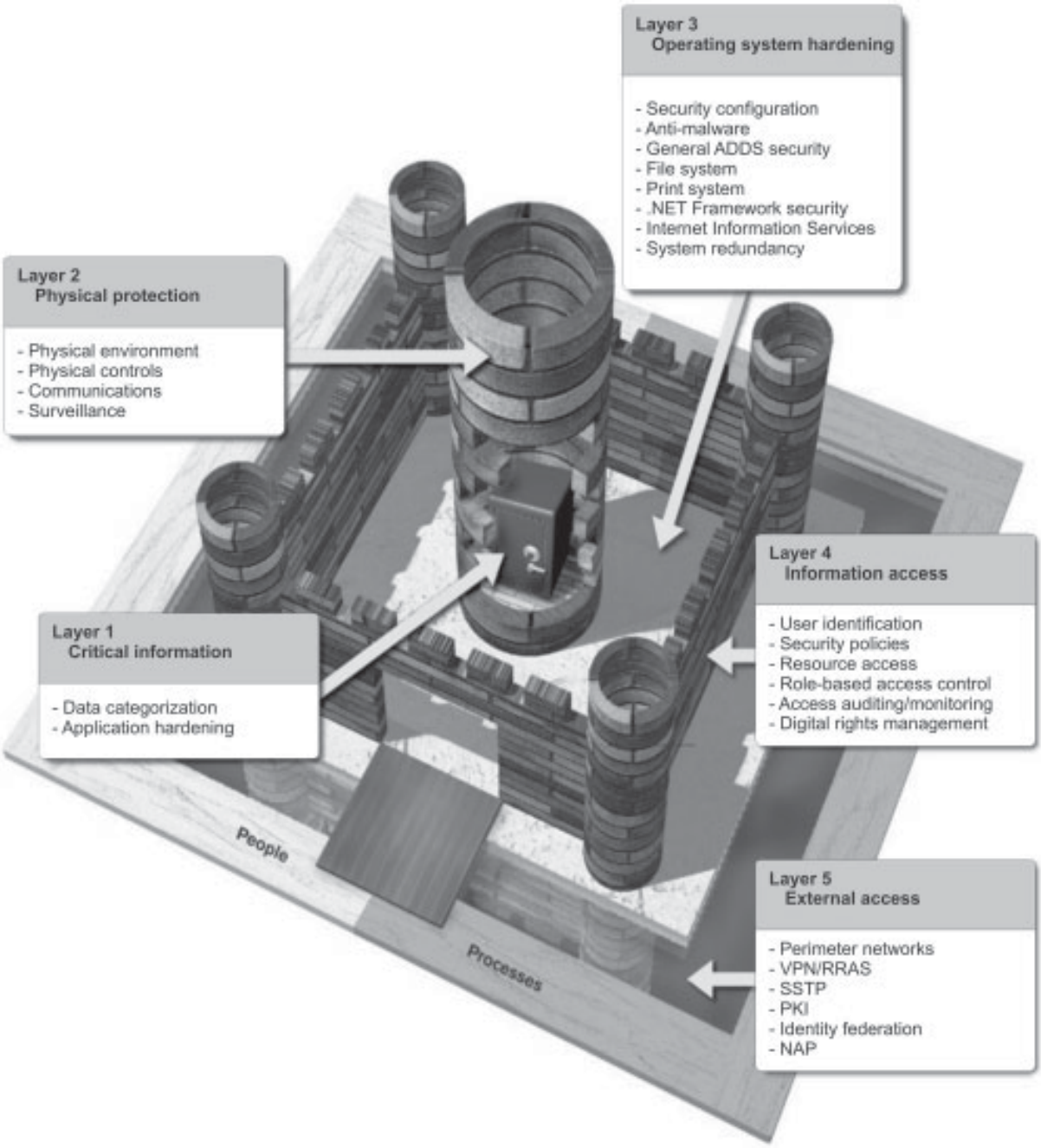
A legjobb módja annak, hogy kialakítsunk egy biztonsági irányvonalat, ha modelleket használunk. A modell, amit dolgozatomban feldolgozni szándékozom a ’CDS’, azaz a ’kastély-védelmi rendszer’.
A középkori időkben, az embereknek meg kellett védeni önmagukat, ingóságaikat egy védekezési formán keresztül, ami elsődlegesen azon alapult, hogy a bejáratokat halmozottan is megvédjük, avagy mai szóval védekezzünk mélységében, több szinten.
Azért használjuk a kastély rendszert, mivel ezt mindenki nagyon könnyen átláthatja, és könnyen megértheti az egyszerű felhasználóktól a szakemberekig. Ha csak egyszer is járt valaki egy középkori kastélyban, vagy csak látott egy filmet, ami kastélyokról szólt, vagy csak beült egy moziba megnézni a Gyűrűk urát, annak emlékeznie kell arra, hogy az első védvonal nagyon gyakran a várárok. A várárkokat azért használták, hogy megállítsák a nem kívánt személyeket abban, hogy elérjék a várfalat. Ezek az árkok gyakran tartalmaztak veszélyes állatokat, ezzel is egy újabb védvonalat kialakítva. A következő védvonal a várfal,

amely teljesen körbevette a kastélyt, és innen könnyen visszaverték az ellenséget. A várfal gyakran lőrésekkel volt ellátva, ahonnan az íjászok könnyedén célba vehették az ellenfelet, miközben ők maguk védve voltak a találatokkal szemben. Aztán a várfalba építve volt egy kapu, felvonóhíddal ellátva. És természetesen mindez belépési pontonként biztonsági őrökkel ellátva. Ha ezeken mind átjutottunk, akkor a várudvarban találjuk magunkat. Ez a 3. védvonal a falakon belül. Ha ide eljut az ellenség, akkor már szemtől szembe kell összecsapni vele.
A 4. védvonal a kastély maga. Ebben találhatóak a korona ékszerek és minden egyes kincs amit meg kell védeni az ellenségtől. Maga a kastély is úgy lett megépítve, hogy védekező funkciót lásson el. A csigalépcsők vékonyak, a szobák úgy vannak kialakítva, hogy megzavarják az ellenséget. Az 5. és egyben az utolsó védvonal a vártorony a kastély szívében. Ezt a legnehezebb elérni, és ez a leginkább védett.
Természetesen ez nem teljes leírása volt egy kastély védelmi rendszerének, de a középkorban nagyon keményen dolgoztak azért, hogy minden egyes védvonalat többszörös védelmi réteggel lássanak el. Egy IT védelmi rendszert hasonlóképpen kellene megtervezni, és hasonlóképpen kellene, hogy kinézzen. Belülről kifelé haladva 5 réteget különböztetünk meg:

1. réteg: **Kritikus információ**: a rendszer szíve, amit meg kell védeni. Ez felel meg a vártoronynak.
2. réteg: **Fizikai védelem**: a biztonság nagysága mindig többszintű fizikai védelemmel kell hogy kezdődjön. Ez felel meg a kastélynak.
3. réteg: **Operációs rendszer megerősítés**: miután a fizikai védelmet megtettük, minden egyes operációs rendszert meg kell szilárdítanunk a külső támadások ellen, amennyire csak lehetséges. Ez felel meg a várudvarnak.
4. réteg: **Információ hozzáférés**: amikor hozzáférést engedélyezünk az adatainkhoz, meg kell bizonyosodjunk abban, hogy mindenki hitelesített, jogosult, és ellenőrzött. Ez felel meg a várfalnak, azaz csak ők jöhetnek keresztül a várkapun.
5. réteg: **Külső hozzáférés**: a védekezés utolsó rétege, ami a külső világhoz kapcsolódik. Ez felel meg a várároknak.

Ezt láthatjuk az 1.1 ábrán.

Természetesen ez csak egy kiinduló pontja annak, amit szeretnénk elérni. Ahhoz hogy a biztonsági irányelveink teljesek legyenek, mindez elengedhetetlen ennek eléréséhez.



1.1 ábra Castle Defense System

Windows Szerver 2008 dióhéjban

Röviden és címszavakban nézzük, mire számíthatunk:

- **szoftveres megszorítások irányelve**, ezek az irányelvek kontrolálják, hogy milyen kódok futhatnak le a hálózatban- alkalmazások, scriptek, batch fájlok – és még korlátozhatják a DLL (Dynamic Link Library)-t is.
- **vezeték nélküli LAN támogatás**
- **távoli hozzáférés hitelesítés**, amely tulajdonság a továbbfejlesztett IAS-en (Internet Authentication Server) és RADIUS (Remote Authentication Dial-in User Server)-en alapszik.
- **NAP** (Network Access Protection)
- **Windows szerver oldali tűzfal,** amely a bejövő és kimenő kommunikációt is megszűri, és tartalmaz egy újdonságot az IPSec-et.
- **PKI (public key infrastructure),** a Windows Szerver 2008 egy továbbfejlesztett PKI-t, és ADCS-t (Active Directory Certificate Services) tartalmaz, ami támogatja az autó-bejegyzést és automatikus X.509 tanúsítvány meghosszabbítást.
- **Web szerver biztonság,** az IIS (Internet Information Services) 7-es verziója.
- **Ideiglenes és offline fájl védelem,** az új SSTP (Secure Sockets Tunneling Protocol)-on keresztül
- **Személyes adatok kezelése,** a Windows Szerver 2008 Credential Manager biztonságosan tudja tárolni a jelszavakat és digitális tanúsítványokat. (X.509)
- **Kernel módú titkosítás,** támogatja az FIPS szabványt (Federal Information Processing Standard), amely egy elfogadott kriptográfiai algoritmus. Ez azt jelenti hogy mind kormányzati és nem kormányzati szervezetek élvezhetik az előnyeit ezen kriptográfiai modulnak a kliens/szerver oldali kommunikációban. Szintén támogatja a Suite B-t.
- **DAP (Digest Authentication Protocol),** egy új biztonsági csomag, amelyet az IIS és a ADDS (Active Directory Domain Services) is támogat.
- **Digitálisan aláírt csomagok**
- **Többszörös jelszó használat**
- **Szerepkör alapú hozzáférés ellenőrzés,** WS08 tartalmaz egy Authorization Manager-t amely támogatja a szerepkör alapú hozzáférés ellenőrzést az alkalmazások

számára. XML (Extensible Markup Language)-ben vagy az Active Directory-ban tárolódnak.

- **Hitelesítés delegálás**, a WS08 támogatja a kényszerített delegálást. Ami azt jelenti, hogy meg lehet határozni, hogy melyik szerverben bízhatunk felhasználói megszemélyesítésben a hálózaton belül. Sőt azt is azonosíthatjuk, hogy a szerver melyik szolgáltatásában bízhatunk.
- **Korlátozott 'Mindenki' tagság**, a Mindenki csoport továbbra is tartalmazza a hitelesített felhasználókat és vendégeket, de az Anonymous csoport tagjai továbbá nem részei a Mindenki csoportnak.
- **Opcionális rész-rendszerek,** mint például a POSIX (támogatja a UNIX alkalmazásokat), nincs alapértelmezettként installálva.
- **Bitenkénti meghajtó tikosítás,** teljes mértékben titkosítani lehet a számítógép meghajtóit, ezzel is fokozni a védelmet
- **Külső eszközök ellenőrzése,** le lehet tiltani az USB meghajtók csatlakoztatását a hálózathoz és a munkaállomásokhoz.

Természetesen ez nem egy teljes listája mindannak, amit a WS2008 nyújtani tud, de a legfontosabb újításokat tartalmazza, ezek közül a legfontosabbakat szeretném megnézni és megismertetni az olvasóval. Ennek ismeretében már lehet tervezni a CDS-t.

1. réteg - Kritikus információ

Az első dolog, amivel kezdenünk kell, hogy meghatározzuk mi az, amit meg kell védenünk. Szervezetek számára nincs választási lehetőség. Együtt működés a hálózaton belüli munka esetén elsődleges hogy adatokat osszanak meg. Gyakran engedélyezni kell, hogy adatokat tároljanak az alkalmazottak a merevlemezeken.

Ehhez az adatokat kategorizálni kell az alábbiak szerint:

- **nyilvános adatok**, mindenki számára elérhető hálózaton belül és kívül egyaránt
- **belső adatok,** olyan információk, amelyek kapcsolatban állnak a szervezet működésével. Lehetnek privát adatok, de nem feltétlenül bizalmasak.
- **bizalmas adatok, o**lyan adatok, amelyeket nem kell vagy nem illik mások tudtára adni. Például személyes adatok, valakinek a fizetése, stb.
- **titkos adatok,** olyan információk, amelyek kritikusak a szervezet működése szempontjából. Ha rossz kezekbe kerülnek, akkor az a szervezetre nézve nagy biztonsági kockázatot jelent.

Minden egyes adat kategóriához meg kell állapítani, hogy melyik elemei azok, amelyek kockázatot jelentenek. Például egy adat a cég weblapján, amit nyilvánosnak vélünk, de a tudtunk nélkül lesz módosítva, azonnal rossz hírnevet eredményezhet a cégre nézve. Ha például az alkalmazottak fizetési adatai kiszivárognak, akkor nem csak az alkalmazottak bizalmát veszítjük el, de elégedetlenséget is kiváltunk.

Az információ 2 elemből áll: adatból és dokumentumokból. Az adat rendszerint strukturált táblákban vagy valamilyen adatbázis típusban, listában tárolódik. A dokumentum strukturálatlan adatokat tartalmaz, és diszkrét objektumokban jelenik meg, mint például szöveg fájlok, kép, hang, videó vagy egyéb dokumentum típusok. Mindkét információ típus védelmet igényel. A dokumentumok védve vannak a tároló rendszer adottságain belül vagy az adatbázis biztonságon keresztül. Illetve a Windows SharePoint Services-en keresztül. Ebben az esetben a dokumentumok adatok lesznek.

2. réteg - Fizikai védelem

A biztonsági vonal 2. rétege a számítógépes rendszer fizikai védelme.
Az alábbiakat kell hogy lefedje, és az alábbi kérdések merülhetnek fel:

- **földrajzi elhelyezkedés:** Környezetileg veszélymentes helyen van-e az épületünk? Van-e bármilyen esélye az árvíznek, lavinának, beomlásnak, amely érintheti az épületünket? Közel vagyunk-e nagy utakhoz, útszakaszokhoz, ahol autóbalesetek veszélyeztethetik a biztonságunkat?
- **társadalmi környezet:** Személyesen meg kell győződni arról, hogy minden időben a számítógépes berendezések biztonságban legyenek. Vigyázni kell arra, hogy a jelszavak semmiképpen se szivárogjanak ki semmilyen körülmények között sem.
- **épület biztonság:** maguk az épületek biztonságosak-e? Bárki, legyen az alkalmazott vagy vendég, aki belép az épületbe annak minden helyiségében azonosítható-e? A vendégek folyamatos felügyelet alatt vannak-e? Működik-e szellőzőrendszer az épületben? Van-e jó tűzvédelmi terve az épületnek? A villanyvezetékek kiépítése biztonságosan történt-e meg, ezzel is csökkentve egy elektromos tűz kockázatának az esélyét?
- **épülettervezés:** az épület tervezése biztonságos-e? Tűzbiztosak-e a falak? Vannak-e tűz gátló ajtók? Vannak-e generátorok a helyiségekben, ha igen, akkor azok védett és biztonságos helyen vannak-e? Vannak-e biztonsági kamerák az illetéktelen behatolók ellen?
- **a szerverek biztonsága:** a szerverszoba kulccsal zárható-e? Az szoba elérhetősége folyamatosan megfigyelhető és ellenőrizhető-e? Maguk a szerverek biztonságban vannak-e? A Windows Szerver 2008 támogatja a smart kártyák használatát az adminisztrátori fiókok esetében. Minden egyes biztonsági környezetben alkalmazni kellene a smart kártyák használatát. Ma már anyagi vonzatai sem annyira magasak és sokkal kevesebb a hátránya, mint előnye ezek alkalmazásának.
- **BIOS (Basic Input Output System) védelem:** Minden egyes számítástechnikai alkatrésznek kellene legyen valamilyen védelmi formája BIOS szinten. A host szerverek esetén ez mindenképpen magában kell hogy foglalja a bekapcsolás utáni jelszó kérést. De ez nem csak a host szerverekre igaz, hanem minden más szerver

esetén is. Az új DMI (Desktop Management Interface) engedélyezi a BIOS jelszavak központosítását is.

- **hálózati biztonság:** a hálózat és a szolgáltatásai biztonságosak-e? Van-e vezeték nélküli hálózat? Az biztonságos-e? Illetéktelen személyek be tudnak-e hatolni a hálózatba?
- **redundancia:** a kritikus rendszer redundáns-e? Illetve ez kiterjedhet az összes érintett rendszerre.

A fizikai védelem minden egyes megjelenése formáját karban kell tartani, és dokumentálni kell. Sőt a lehető legrészletesebb formában közölni kell az alkalmazottak felé. Az alkalmazottaknak tudatában kell legyenek annak, hogy ők azok akik tudnak és akiknek részt kell vállalni minden egyes gyanús cselekmény felderítésében ezzel is hozzájárulva a biztonság minden szintű megőrzéséhez.

3. réteg - Operációs rendszer megerősítés

Az operációs rendszer megerősítésnek a célja, hogy lecsökkentsük a lehetséges támadási pontokat. Hogy ezt megtegyük először is el kell távolítsunk mindent, amit nem igényel a rendszerünk. A Windows Szerver 2008 ebben nagyon jó, mivel már a kezdetekkor csak a központi komponenseket installálja fel, és ezt követően nekünk van lehetőségünk a további szolgáltatások telepítésére. Azonkívül, az IIS nincs installálva alapbeállításként, így azok a rendszerek, amelyeknek nincs rá szükségük, nem is tartalmazzák azt.
Azonban nem csak a szolgáltatások számbeli korlátozása az egyetlen dolog, amit tennünk kell, figyelmet kell fordítani a következőkre is:

- rendszer biztonsági beállítások
- a megelőzés stratégia
- ADDS (Active Directory Domain Services) biztonság
- fájl rendszer biztonság
- nyomtató rendszer biztonság
- .NET keretrendszer biztonsága
- IIS biztonság
- rendszer redundancia

3.1 Rendszer biztonsági beállítások

A rendszer biztonsági beállításokat 2 szinten kell végrehajtanunk. Az első szint a telepítés utáni konfiguráció-módosításokra fókuszál. A második szint magába foglalja a biztonsági sablonokat egyetértésben a szerver oldali szerepkörrel. Ez nagyban támaszkodik a Biztonsági Konfiguráció Varázslóra (Security Configuration Wizard), amely automatikusan alkalmazza a beállításokat a rendszerünkre.
Telepítés utáni biztonsági lista, amely a következőket foglalja magában.

- Nevezzük át az adminisztrátori fiókot. Alkalmazzunk komplex fiók nevet és jelszavat. A komplex jelszavak az egyik legjobb védekezési rendszerünk. A 15 karakterből álló jelszavak, - a Windows felkínálja mind a 127 karaktert - amelyek tartalmaznak kis és nagybetűket, számokat, és speciális karaktereket majdnem feltörhetetlenek. Az ismert jelszó feltörő rendszerek csak abban az esetben működnek, ha 14 vagy kevesebb karakterből áll a feltörni kívánt karaktersorozat.

- Másoljuk át az adminisztrátori fiókot, és ezzel hozzunk létre egy biztonsági másolati fiókot (backup account). Ne felejtsük el a komplex fióknév és jelszó használatát.
- Ekkor hozzunk létre egy ál-adminisztrátori fiókot. Mindez csapdaként szolgáljon azok számára, aki a valódi adminisztrátori fiókot szeretnék elérni. Ellenőrizzük a belépéseket ezzel kiszűrve, hogy ki az, aki megpróbált behatolni a rendszerbe.
- Bizonyosodjunk meg arról, hogy a 'Belépés vendégként' fiók ki van kapcsolva.
- Ellenőrizzük a futó szolgáltatások listáját és bizonyosodjunk meg benne, hogy mindegyikük jól dokumentálva van. A szükségtelen szolgáltatásokat állítsuk le.
- Ellenőrizzük a nyitott portok listáját és zárjuk le a szükségtelen portokat. A nyitott portok listáját a NETSTAT paranccsal tehetjük meg:

  ```
  netstat -a -n -o
  ```

  Az –a kapcsoló az összes portot hívja meg, az –n a port számát, míg az –o a porthoz társított folyamatot.

Habár a komplex jelszavak használata az egyik legjobb védekezési forma, ugyanakkor ez lehet az egyik rémálmunk is, mivel a komplex jelszavakat elég nehéz fejben tartani. Az egyik megoldás lehet az, ha megpróbálunk teljes szavakat vagy kifejezéseket használni, miközben betűket cserélünk ki számokra és speciális karakterekre.
Például egy egyszerű **adminisztrátor** szó helyett használhatjuk a következőt:
Ad/\/\1n1$Tr4T0r.
Természetesen. ha lehet ne használjuk ugyanazt a jelszót több helyen. Illetve ha valakinek nehézséget okoz a komplex jelszavak megjegyzése, akkor használjon jelszó tároló eszközöket, és ebben az esetben csak egy komplex jelszót kell megjegyeznünk, mivel az összes jelszavunkat egy titkosított fájl tartalmazza.

3.2 Rendszerleíró adatbázis (Registry), fájlrendszer és rendszer szolgáltatások biztonsága

A Registry vagy magyarul rendszerleíró-adatbázis tárolja a számítógép konfigurációs és a Windows működéséhez szükséges adatait. Sokan idegenkednek a használatától, mely érthető, hiszen a rendszer szempontjából kulcsfontosságú adatokat tárol, és egy rossz mozdulattal hatalmas károkat lehet okozni.

Néhány jó tanács:

- A Registry amennyire csak lehet stabil, és megerősített legyen. Először is gondoskodjunk arról, hogy a hozzáférés kontrolálva legyen a registry editorhoz, azaz a rendszerleíró adatbázis szerkesztőjéhez. Ezt elérhetjük a REGEDT32.EXE és a REGEDIT.EXE fájlok hozzáférésének a korlátozásával. Ezek a beállítások a Felhasználói Konfiguráció / Szabályok / Adminisztratív sablonok / Rendszer alatt találhatók.
- Következő lépésben biztosítsuk a kulcsokat magában az adatbázisban. A legegyszerűbb módja ennek, ha kiterjesztjük a hozzáférést az öröklődés által a szülő kulcsokról a gyerekkulcsok felé. Előfordulhat azonban hogy ez nem mindig elvégezhető.
- Szintén biztosíthatjuk a fájlokat és a könyvtárakat. De legyünk figyelmesek, mivel egyes fájlok a Windows Szerver 2008 által automatikusan már védve vannak, így ha módosítjuk a biztonsági beállításokat, akkor azokat felülírjuk és nem biztos, hogy mindig a megfelelő irányba teszzük.
- Végül beállíthatjuk, hogy mely modulok induljanak el a rendszerünk indulásakor. Ezeket 4 csoportba soroljuk:
  - **Automatikusan induló modulok**, amelyek szükségesek a rendszer indulásához
  - **Automatikusan, de késleltetve induló modulok**, amelyek elindulnak ugyan automatikusan, de nem szükségesek a rendszer indulásához.
  - **Kézi indítású modulok**, amelyek vagy felhasználó által, vagy egy szolgáltatás által lesznek aktívak, de nem szükségesek, hogy a rendszer indításkor automatikusan elinduljanak.
  - **Inaktív modulok,** amelyek nem szükségesek a rendszerünk indulásakor.

3.3 Biztonsági sablonok

A GPO (Group Policy Objects) biztonsági beállításai 3 helyen vannak eltárolva a Windows Szerver 2008-ban. Az első maga a GPO a Policies/Windows Beállítások/Biztonsági Beállítások menüpontban találhatók mind a rendszer, mind a felhasználói beállítások számára. A második lehetőség egy biztonsági sablon fájl. A legtöbb esetben ez az egyik legjobb módszer, mivel automatikusan létrejön egy biztonsági fájl, amely tartalmazza a beállításokat.

A harmadik lehetőség megengedi a számunkra, hogy egy mindent átfogó szabályrendszert alkossunk a Biztonsági Konfiguráció Varázslón (Security Configuration Wizard) keresztül.

Számos lehetőség közül választhatunk, ha alkalmazni szeretnénk egy biztonsági sablont. Első lehetőség a GPO-n keresztül való importálás. Ezt megtehetjük az alábbi módon: a Szerkesztő menüben az egérrel történő jobb-kattintást követően, ha kiválasztjuk az 'Import policy ' opciót, akkor kapunk egy párbeszéd panelt, ahonnan kiválaszthatjuk az elérhető sablonokat. Az importált sablonokat hozzáfűzhetjük a meglévő biztonsági beállításokhoz vagy teljesen lecserélhetjük azokat.
A második lehetőség a Biztonsági Konfiguráció Varázsló használata. Ezen eszköz segítségével előbb létrehozhatunk egy sablont, majd ezt a sablont alkalmazhatjuk az összes többi szerveren. Az alábbi biztonsági területeket érhetjük el a Varázsló használatával:

- Felhasználói fiókok szabályrendszere. Jelszó, zárolás, Kerberos.
- Helyi szabályok. Ellenőrzés, felhasználói feladatok, és biztonsági opciók.
- Események naplózása. A rendszer, az alkalmazások, biztonság, könyvtár, fájlmásolat, és DNS szolgáltatások naplózása.
- Korlátozott csoportok.
- Rendszerszolgáltatások. Induló modulok és szolgáltatások.
- Fájl rendszer. Hozzáférés a könyvtárakhoz és fájlokhoz az új NTFS (New Technology File System) rendszeren keresztül.
- Vezetékes hálózati szabályrendszer(IEEE 802.3)
- Windows Tűzfal kibővített biztonsági opcióval
- Vezeték nélküli hálózati szabályrendszer (IEEE 802.11)
- Szoftveres megszorítások szabályrendszere. Korlátozza, hogy melyik program futhat és melyik nem a hálózatban.
- NAP (Network Access Protection)
- IP biztonsági szabályok Active Directory-nál. Kliensek és szerverek közötti kommunikációs beállítások.

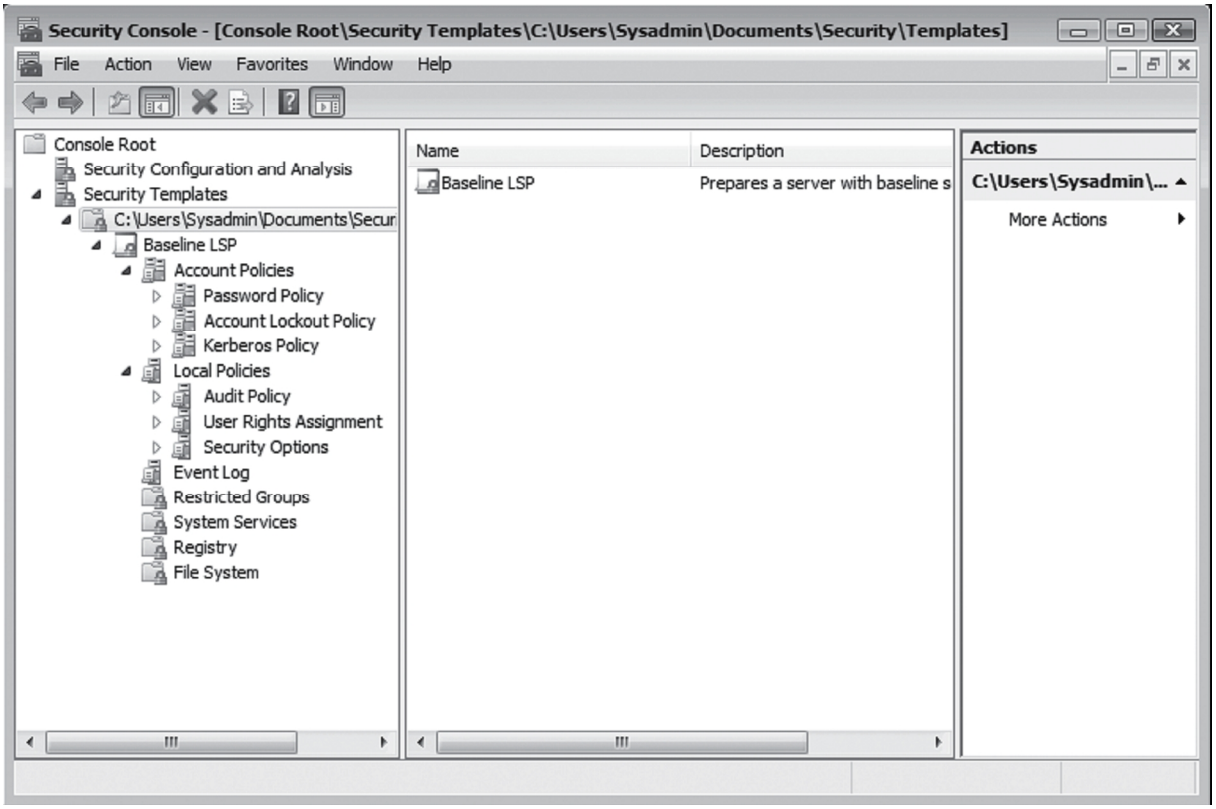
Fontos azonban megjegyezni, hogy meggondolatlan biztonsági sablonok, amelyekkel nem vagyunk teljesen tisztában, súlyos sérüléseket okozhatnak a rendszerben. Mivel a sablonok

módosítani fogják az alap biztonsági beállításokat, ezért érdemes egy tesztkörnyezetben kipróbálni őket, mielőtt élesben alkalmaznánk a rendszerben.

3.4 Biztonsági sablon létrehozása

Az első dolog, amit tennünk kell, hogy létrehozunk egy Biztonsági Sablon és Konfigurációs konzolt, mivel egyetlen konzol sem elérhető alapbeállításként. Ezt a következőképpen tehetjük meg:

1. Válasszuk a Start menü Futtatás parancsát, ahol gépeljük be az MMC mozaik szót.
1. Ekkor elindul a Microsoft Management Consol-ja, ahol a File menü Add/Remove Snap-in parancsát választva kapunk egy párbeszédpanelt.
2. Itt válasszuk ki a Biztonsági Sablonok-at és adjuk hozzá a Hozzáad gomb segítségével. Majd ismételjük meg a Konfiguráció és Analízis esetén is. Majd nyomjuk egy OK-t és visszatérünk magába a konzolba. Majd a File menü Mentés másként parancsa segítségével mentsük el Biztonsági Konzol néven.(Lásd 3.4 ábra)
3. Ezen konzol segítségével hozzáadhatjuk a saját sablonjainkat. Alapbeállításként, az új sablonok a Dokumentumok / Biztonság / Sablonok alatt vannak eltárolva. A létrehozáshoz kattintsunk jobb klikkel a könyvtár nevén, majd válasszuk az Új sablont. Adjunk neki nevet, és leírást. Ne feledjük, hogy később részletesen meg kell adnunk a pontos beállításokat.
4. Ahhoz hogy beállítsuk a rendszerleíró- adatbázis biztonságát, kattintsuk jobb klikkel a Registry-n, majd a dialógus ablakban válasszuk ki a megfelelő kulcsot, amit szeretnénk biztosítani, és nyomjunk OK-t. Itt eldönthetjük, hogy alkalmazni akarjuk-e a gyerekkulcsokra is. Ezt ismételjük meg az összes szükséges kulcsra.
5. A fájl és könyvtárak biztonságát elvégezhetjük az alábbi módon. Jobb klikk a Fájlrendszeren, és válasszuk ki a Fájlt hozzáad… opciót. A megfelelő fájlok kiválasztása után nyomjuk OK-t.



3.4 ábra Biztonsági Konzol

3.5 Helyi biztonsági sablonok

A helyi biztonsági sablonokat kétféleképpen tudjuk alkalmazni: vagy a grafikus felületű Biztonsági Konfiguráció és Analízis nevű eszköz segítségével vagy a parancssoros üzemmódú SECEDIT eszköz segítségével. Mindkettőnek megvannak az előnyei. Mindkettőt biztonsági sablonon alapuló elemzésre és beállításra lehet használni.

Ha az első eszköz segítségével szeretnénk elemezni a számítógépünket, és összehasonlítani egy adott biztonsági irányvonallal, akkor a következőt kell tennünk.

1. Jobb klikk a Biztonsági Konfiguráció és Analízis-re a biztonsági konzolon belül, majd válasszuk az Adatbázis választása opciót.
2. Az Adatbázis választása párbeszéd panelben vagy a meglévő adatbázisokból választunk vagy megadhatjuk az új adatbázis nevét, majd nyomjunk egy OK-t. A meglévő adatbázisokat a Dokumentumok / Biztonság / Adatbázisok elérési út alatt találhatóak.
3. Majd ki kell választanunk azt a sablont, amit használni szeretnénk az elemzésre. Ezt a sablont már korábban elkészítettük. Válasszuk ki ezt és nyomjunk OK-t.

4. Ha azonnal szeretnénk elemzést végezni, akkor nyomjunk jobb klikket a Biztonsági Konfiguráció és Analízisen, majd válasszuk az Elemzés azonnal opciót.
5. Mivel minden művelethez szükség van egy LOG fájlra, ezért egy felugró ablakban meg kell adnunk ennek a helyét, hogy hol található. Az alap elérési út a Dokumentumok / Biztonság / Log fájlok és az alap fájl név megegyezik az adatbázis nevével. Itt választhatunk, hogy új nevet adunk meg, vagy használjuk a Keresés opciót, amellyel meglévőt választunk ki, vagy egyszerűen elfogadjuk az alapbeállításként felajánlott log fájlt.
6. Ekkor elkezdődik az elemzés, és amint ez befejeződik, azonnal láthatjuk a beállítási különbségeket a sablon és a számítógép között. Egyszerűen csak rá kell állnunk arra a beállításra, amelyet látni szeretnénk. Ezt a jobb oldalon részletezve olvashatjuk.
7. Szintén megnézhetjük a log fájl tartalmát. Ehhez nyomjunk jobb klikket a Biztonsági Konfiguráció és Analízisen és válasszuk a Log fájl megtekintése opciót. Ekkor a log fájl tartalmát a jobb oldali panelen láthatjuk.
8. Módosíthatjuk az adatokat ahhoz, hogy összhangba hozzuk azzal az értékkel, amit mi szeretnénk. Ezt megtehetjük dupla kattintással a megfelelő értéken, majd mentés előtt válaszuk az Alkalmazzuk az új értékeket opciót.
9. Majd jobb klikk a Biztonsági Konfiguráció és Analízis panelen, és Mentés opció. Ezzel elmentettük a kívánt változtatásokat.
10. Hogy elvégezzük a számítógép konfigurálását az adatbázis legújabb beállításaival, válasszuk a Számítógép konfigurálása azonnal opciót.
11. Majd amint végeztünk zárjuk be a biztonsági konzolt.

A másik módszer a SECEDIT (Windows Security Configuration Editor Command Tool) használata lehet. Egy tipikus parancs az alábbi módon kell, hogy kinézzen:
`secedit /configure /db` ***filename*** `.sdb /log` ***filename*** `.log`

Lehetőségünk van részletesebb log fájl létrehozására is az alábbi kapcsolóval: `/verbose`
Amennyiben nincs beállítva log fájl, abban az esetben a SECEDIT automatikusan ment mindent a SCESRV.LOG nevű fájlba. Mivel a helyi biztonsági sablonok csak a fájl rendszert, a rendszerleíró-adatbázist, és a rendszerszolgáltatásokat érintik, ezért meg kell

bizonyosodni arról hogy a parancs csak a sablon ezen részeire vonatkozik. Ehhez használjuk a következő parancsot:

```
secedit /configure /db filename.sdb /log filename.log /areas
REGKEYS  FILESTORE SERVICES /quiet
```

A SECEDIT nagyon hasznos lehet az általános biztonsági beállítások ellenőrzéséhez is, mivel tartalmazza a `/analyze` kapcsolót. Mind az elemzést, mind a konfigurációt automatizálni lehet a Feladat Ütemezőn keresztül, ami a Vezérlőközpontban található.

Ha többet szeretnénk megtudni a SECEDIT-ről, akkor olvassuk el a Súgót, vagy csak egyszerűen gépeljük be `secedit` parancsszót a Futtatás menübe.

3.6 Biztonsági Konfiguráció Varázsló (Security Configuration Wizard)

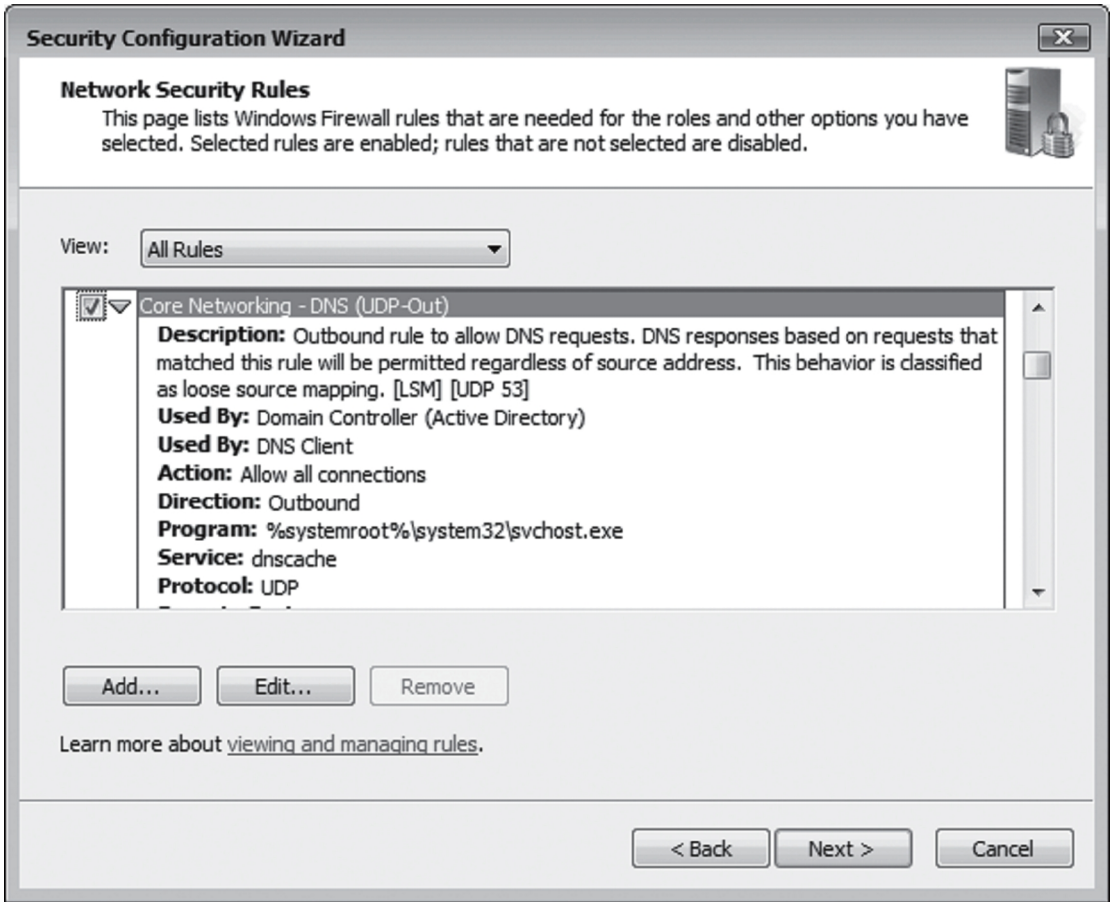
A biztonsági sablonok nagyon hasznosak, azonban a Windows Szerver 2008 egy sokkal hatékonyabb eszközt kínál számunkra, a Biztonsági Konfiguráció Varázslót. (Lásd 3.6 ábra) Segítségével az alábbiakat tehetjük meg:

- Szigorúbb szolgáltatás konfiguráció a szerepkör-alapú konfigurációkon keresztül
- Szigorúbb hálózati biztonság
- Szigorúbb rendszerleíró-adatbázis beállítások
- Megvalósít egy ellenőrző politikát

Ezeket alap elérhető szolgáltatásként találjuk meg a Varázslóban. Azon felül lehetőségünk van az IIS (Internet Information Services) biztonsági beállításait is elérni. Az egyik legjobb része a Varázslónak, hogy teljes körű magyarázatot kapunk mindenre. Hogy mit módosítunk, és az a módosítás pontosan milyen következménnyel jár. A Biztonsági Konfiguráció Varázsló működik parancssoros üzemmódban is, ez a SCWCMD.EXE. Azonban az output XML formátumban készül el, ami alapból inkompatibilis a GPO-val (Group Policy Object). Ahhoz hogy olvasható formátumba hozzuk, szükségünk van a következő parancsra:

```
scwcmd transform /p:PolicyFile.xml /g:GPOName
```

Segítségével az XML fájlból egy új GPO objektumot hozunk létre, amit csak adminisztrátori jogkörrel lehet futtatnunk. A szabályrendszerek a `%SYSTEMROOT% \SECURITY \MSSCW \POLICIES` mappába kerülnek elmentésre.



3.6 ábra Biztonsági Konfiguráció Varázsló

3.7 Eszköz Vezérlő (Device Control)

A Windows Vista egy teljesen új dolgot hozott a Windows operációs rendszerek életébe: a lehetőséget a hordozható eszközök konfigurálására a Group Policy használatán keresztül. Eldönthetjük, hogy milyen hordozható eszközöket engedünk csatlakozni a rendszerünkhöz és milyeneket nem. Ezzel könnyen elkerülhetjük, hogy egy rosszindulatú felhasználó csak úgy kisétálhasson fontos információkkal, amelyeket egy egyszerű hordozható eszköz csatlakozásával, és adatokat arra történő lementésével ért el.

Általánosságban készítünk egy jóváhagyott listát az eszközeinkről és elhelyezzük ezt a GPO-ban. Például megengedjük a felhasználóknak, hogy USB egereket és billentyűzetet csatlakoztassanak a rendszerünkhöz, de tiltjuk a memória kártyák és hasonló eszközök csatlakozását. Ilyenek lehetnek az Apple iPod-ok, amelyek igen csak nagy információ

tárolására alkalmasak, főleg a legújabb modellek. Vagy például a zseb számítógépek (pocket PC), vagy az okos kis telefonok (smart phones).
Ne feledjük a legjobb védekezés a teljes védekezés!

3.8 BitLocker Teljes Meghajtó Titkosítás

A Windows Vista megjelenésével a Microsoft bemutatta a BitLocker Teljes Meghajtó Titkosító alkalmazását is. A BitLocker segítségével titkosítjuk az operációs rendszer köteteinek tartalmát, így megelőzve, hogy illetéktelen felhasználók elérjék azt. A BitLocker főleg mobil eszközök esetében használjuk, illetve olyan eszközök esetében, amelyek igen érzékeny adatokat tartalmaznak. Szintén alkalmazzák a szerverek meghajtóinak a titkosítására is, mivel a Windows Szerver 2008 támogatja ezt a lehetőséget. Sőt ha akarjuk, alkalmazhatjuk az összes virtuális gépünkre is, mivel ha valaki el is tulajdonít egy fájlt a gépről, képtelen lesz annak használatára.
Ahhoz hogy képesek legyünk használni a BitLocker előnyeit, a rendszerünknek a következőkkel kell rendelkeznie.

- 2 partíciót kell tartalmaznia. Egyet a rendszer köteteinek, egyet az operációs rendszer köteteinek. A rendszer köteteinek szükségük van legalább 1,5 GB tárhelyre, mivel ez a partíció tartalmazza majd a boot-oláshoz szükséges köteteket.
- Szükségünk van egy USB meghajtóra, illetve egy olyan BIOS-ra, amely támogatja az USB meghajtó írását és olvasását az induláskor.
- Ideális esetben tartalmaz egy TPM (Trusted Protection Module)1.2 microchip-et.
- Illetve egy TCG (Trusted Computing Group)–szolgálatkész BIOS-t.

Láthatjuk, hogy a BitLocker futtatásához egy külső USB meghajtó szükséges. Ezen a meghajtón tároljuk a titkosító kulcsot, aminek a segítségével blokkolhatjuk vagy feloldhatjuk az operációs rendszer partícióját. A mások oldalról nézve, viszont egy USB meghajtó használata kockázatot jelent, mivel könnyen elveszíthetjük vagy ellophatják tőlünk. Ezért is ideális, ha olyan szervert használunk, amely tartalmazza a teljes TPM komponenseket. Ilyen esetekben a titkosító kulcs biztonságban tudható a microchip által, és nem tudjuk elveszíteni, illetve így a lopást is kiküszöbölhetjük.
A BitLocker használatához a következő eljárást kell követnünk:

- Kezdéshez az installálás alatt 2 partíciót kell létrehoznunk. Mindkét partíció elsődleges partíció kell hogy legyen. A kisebb partíció legyen az aktív partíció. Mindkét partíció NTFS formattáláson kell hogy átessen.
- Installáljuk fel a Szerver Core-t az operációs rendszer patícióra.
- Miután ezzel végeztünk, hajtsuk végre az installálás utáni konfigurációkat.
- A következő lépés a BitLocker installálása:

```
start /w ocsetup BitLocker
```

  Miután végeztünk, indítsuk újra a rendszert.
- Ha a rendszer újraindult, készen állunk a BitLocker konfigurálására. Kezdésnek listázzuk ki a kompatíbilis meghajtók neveit. Mindezt a megfelelő mappában tegyük.

```
cd\windows\system32
cscript manage-bde.wsf –status
```

- Így készen állunk a rendszermeghajtó titkosítására az alábbi paranccsal:

```
cscript manage-bde.wsf –on C: -RecoveryPassword
```
NumericalKey `–RecoveryKey` *BitLockerDrive* `–StartupKey` *BitLockerDrive*

  A *BitLockerDrive* annak a meghajtónak a jele, amelyet a partíciónak adtunk.
  A *NumericalKey* egy 48számjegyből álló számsorozat. 8darab 6os csoportra osztva, kötőjelekkel elválasztva. Mind a 8 csoport osztható kell legyen 11-el, és nem lehet nagyobb mint 720896. / 720896:11=65536, ami 2^{16} /
- Megismételhetjük ezt a parancsot, amennyiben más meghajtót is szeretnénk titkosítani.

Mint látjuk ez egy egyszerű parancs nagyon hatásos eredménnyel. Természetesen tudjuk biztonságban mind a titkosító kulcsot, mind a helyreállító jelszót.

3.9 A rosszindulatú programok elleni védelem

Egy másik nagyon fontos védelmi réteg a rosszindulatú programok elleni védekezés, azaz az anti-malware stratégia. Ahhoz hogy létrehozzunk egy teljes körű védelmi rendszert, elengedhetetlen az anti-vírusok, anti-kémprogramok, anti-spam eszközök, és általános anti-malware eszközök használata. Habár ez nem egy Windows Szerver 2008 funkció, de a WS2008 nagyon sok API-t (application programming interface) bocsát a rendelkezésünkre, amely segítségével átvizsgálhatjuk rendszereink fájljait és objektumait. Beépített programként találjuk meg a Windows Defender-t, illetve az ingyenes Anti- Spyware programot, de ezek önmagukban nem elegendőek. Ezért is dolgozik a Microsoft széleskörűen annyi anti-malware eszközgyártóval, hogy biztos legyen abban, hogy a termékük nagyon jól képes működni stresszes környezetben, illetve nagy nyomás alatt is a Windows operációs rendszerrel.
Egy teljes anti-malware stratégiának a következő elemeket kellene tartalmaznia:

- Központi intézkedést mind a kliensekre, mind a szerverekre
- Automatikus telepítéseket a kliens és szerver gépekre
- A Microsoft Management Consol (MMC) az adminisztrációs feladatokhoz
- Automatikus letöltést az új anti-malware aláírások esetében
- Eltérő letöltési időpontokat, hogy elosszuk a munkaterhelődést
- Automatikus aláírás telepítéseket mind egyes kliensre
- Automatikus rendszerszűréseket és átvizsgálásokat
- A vizsgálati eredmények központi kollekcióban való tárolását
- Egy felbukkanó rosszindulatú program esetén azonnali riasztás küldését
- A teljes eltávolíthatóság lehetőségét
- Az azonosított programok központi karanténba helyezését, majd a rendszer automatikus megtisztítását
- Felfedezni a szokatlan viselkedéseket, és ezzel behatárolni az esetleges rosszindulatú programok helyzetét
- Az e-mailek és adatbázisok ellenőrzésének támogatása
- Támogatás és segítség a gyártóktól

Az egyik legjobb megoldás ma a piacon a Symantec Corporation Endpoint Security programja. Annyira egyszerű telepíteni, hogy egy adminisztrátor, akinek semmilyen tapasztalata sincs, 1 órán belül végez mindennel. Miután megtörtént a telepítés, nyugodtan

hátradőlhetünk, mivel semmilyen dolgunk sincs. A program önmagát telepíteni az összes kapcsolódó rendszerre, és automatikusan végzi el a frissítéseket is.
Bármilyen megoldást is választunk, ne feledkezzünk el arról, hogy csak akkor csatlakozzunk a külvilágra, ha már teljes mértékben meggyőződtünk a program helyes működésében.

3.10 Szoftveres megszorítások politikája

Az anti-malware stratégia nem lehet teljes a Windows Szerver 2008 és a Group Policy támogatása nélkül. A WS2008 tartalmazza a GPO beállítások egy speciális halmazát, amely azonosítja azokat a kódokat, amelyek engedéllyel futtathatók és operálnak a hálózaton belül. Ezeket hívjuk szoftveres megszorítások politikájának (SMP). Ennek segítségével szűrhetjük ki az ismeretlen kódokat, és tilthatjuk azok futását. Habár ennek segítségével, mintegy 38 fajta fájltípust kontrollálhatunk – tulajdonképpen bármit, ami kódnak néz ki – mégis van 2, amire nagyon komolyan oda kell figyelnünk. Ezek a szkriptek és a makrók. A legtöbb fenyegetés ezen 2 fájltípus egyikének az alakjában érkezik. Mivel mi magunk vagyunk azok, akik kontrolláljuk azt, hogy mi történjen a hálózatunkban. Ezért explicit módon meg kellene tudnunk mondani, hogy melyek azok a makrók és szkriptek, amelyek az engedélyünkkel futhatnak. A legegyszerűbb módja mindennek, ha digitálisan aláírjuk a szkripteket és a makrókat. Az aláírásokat egy PKI igazolással a kódban helyezhetjük el. Ezt követően megadhatjuk azt az SMP-t, ami majd tiltani fogja azon kódok futását, amelyek nem rendelkeznek ezzel a digitális aláírással. Az SMP-ket a Computer Configuration | Policies | Windows Settings | Security Settings | Software Restriction Policies mappában találjuk. Alapbeállításként ez a mappa üres. Kezdéshez ki kell választanunk az Új Szoftveres Megszorítás Létrehozása lehetőséget. Majd lehetőségünk van azonosítani azokat a kiterjesztéseket, amelyeket tiltani szeretnénk.

3.11 Engedélyek, tiltások és hatásaik

Az engedélyeket 2-féle csoportba sorolhatjuk: explicit engedélyek és öröklött engedélyek. A Windows Szerver 2008 új NTFS (New Technology File System) fájlrendszere is alkalmazza a biztonsági öröklődés fogalmát. Ez azt jelenti, hogy minden gyermek objektum örökli a szülő objektum biztonsági beállításait. Azonban ami új és különleges, az öröklődés módja. Az explicit engedélyek felülírják az öröklött engedélyeket, még akkor is, ha azok nem engedélyek, hanem tiltások (deny permission). Konkrétan ez azt jelenti, hogy lehetséges

definiálni egy tiltást egy szülő objektumon, majd definiálni egy engedélyt (allow permission) annak gyermek objektumán.
A könyvtárszerkezet 2-szintű engedélyezést vagy tiltást kínál fel a számunkra. Az első szintet elérhetjük, ha bármely objektumon az egér jobb klikkjével előhívjuk a helyi menüt, és kiválasztjuk a Tulajdonságok opciót. Itt az alábbi fülek közül választhatunk:

- általános (general)
- megosztás (sharing)
- biztonság (security)
- testreszabás (customize)

A biztonság fület kiválasztva, külön-külön állíthatjuk be felhasználókra lebontva a könyvtár összes tartalmára csoportosítva a különböző jogosultságokat.

- teljes (full control),
- módosítási (modify),
- olvasási és futtatási (read&execute),
- listázási (list folder contents),
- írási (write),
- olvasási (read),
- különleges engedélyek (special permissions).

A második szintet a Speciális gombra kattintva érhetjük el. Itt egy újabb párbeszédpanelt kapunk a következő fülekkel:

- engedélyek (permissions)
- ellenőrzés (auditing)
- tulajdonos (owner)
- hatékony engedélyek (effective permissions)

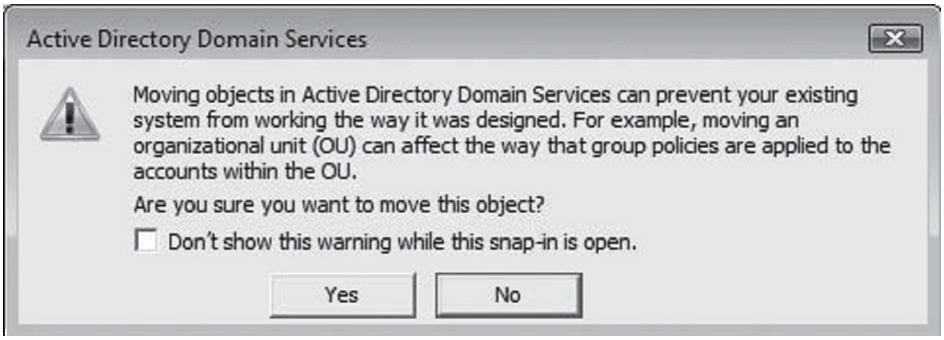
Mindegyik fül segítségével tovább operálhatunk az engedélyekkel, a hatékony engedélyek segítségével pedig tovább szigoríthatjuk a már meglévő jogosultságokat.
Az egyik legjobb tanács és alkalmazott taktika lehet, hogy nem külön felhasznlókra vonatkoztatjuk az engedélyeket, hanem csoportokra. Így sokkal hatékonyabbak lehetünk.

3.12 ADDS (Active Directory Domain Services) auditálás

A Windows operációs rendszerek a Windows 2000 megjelenése óta támogatják az ADDS események ellenőrzését, avagy auditálását. Az ellenőrzött események alapbeállításként az Esemény Naplózóban (Event Log) kerülnek eltárolásra, azonban ezek sok kívánni valót hagynak maguk mögött. Mivel csak annyi információt közölnek velünk, hogy egy objektumon történt-e változás és semmi mást. A Windows Szerver 2008 megjelenésével azonban ez is fejlődött. Már nem csak azt tekinthetjük meg, hogy egy objektumon történt-e változás, hanem azt is, hogy milyen érték változott, és mi volt azt megelőző érték. Sőt lehetőségünk van arra, hogy visszaállítsuk az értékeket a megelőző értékekre.

A könyvtárak azonban nagyon érzékeny környezetek. A Windows 2000-ben például nem volt nyomkövetés vagy figyelmeztetés, amikor egy operátor elvégzett egy módosítást, például objektumokat helyezett át. Egyébként az objektumok áthelyezése egy elég trükkös dolog az ADDS-ben, mivel a rendszer viselkedésének megváltozásához is vezethet. A Microsoft ezért egy újdonságot vezetett be a Windows Szerver 2003 esetében. Minden egyes objektum átmozgatás esetében egy figyelmeztetés jelenik meg az operátor számára, aki eldöntheti, hogy folytatja a megkezdett műveletet vagy visszahátrál attól. (Lásd 3.12 ábra). Azonban volt egy hátulütője a dolognak, az hogy az operátorok akár ki is kapcsolhatták ezt a funkciót, ezzel tulajdonképpen elérve a korábbi Windows 2000-es beállításokat.

A Microsoft a Windows Szerver 2008-ban azonban egy újabb lépést tett előre a biztonság érdekében. Hozzáadtak egy új védelmi eszközt az objektumok létrehozásakor az ADDS-ben. Minden objektum alapbeállításként védve van a törléstől. Persze ez azt is jelenti, hogy az átmozgatástól is. Így minden alkalommal be kell lépnünk a helyi menü Tulajdonságok részébe, és ott a Speciális gombra kattintva ki kell ezt kapcsolnunk. Azonban ez a hosszúnak tűnő műveletsorozat önmagában még nem elegendő. Még be kell kapcsolnunk az ADDS auditálást is. Ez egy 2 lépéses folyamat. Első lépésként bekapcsoljuk az auditálást a megfelelő GPO-ban, majd második lépésként meghatározzuk, hogy melyik objektumot kitől kell ellenőrizni.



3.12.ábra ADDS figyelmeztetés

3.13 Fájl rendszer biztonság

A fájl rendszer egy nagyon fontos része az operációs rendszer megerősítésének. Az NTFS rendszer egy nagyon fontos és lényeges pillére a CDS (Castle Defense System)-nek. Minden lemez és fájl védelmi mechanizmus azon alapszik, hogy az NTFS rendszer adottságait mennyire használjuk ki. Ugyanez vonatkozik a fájlok titkosítására is. Ha nincs NTFS, nincs titkosítás sem. Az egyik legfontosabb szempont a fájlrendszer biztonságát illetően a képesség arra, hogy naplózzunk minden egyes fájlon történő változást, és értesítsük a szervezetet, ha engedély nélküli változtatás történt. Ezt megtehetjük a fájl hozzáférések ellenőrzésének a módjával, de néhány kritikus esetben jobb, ha eszközöket használunk minderre. Az egyik ilyen eszköz lehet ma a piacon a Tripwire for Server. A Tripwire nyomon követ minden egyes fájlon történő változást, és azonnal értesíti az adminisztrátorokat, amikor kritikus fájlok módosultak illetéktelen személyek által.
Sőt, a fájlrendszer biztonság jelentős mértékben nőtt a Windows Szerver 2008-ban. Elég erős biztonsági megszorításokat alkalmaz például a Felhasználók csoportjára. Például a felhasználók nem futtathatnak olyan alkalmazásokat, amelyek olyan fájlokat módosítanának, amelyek érzékeny könyvtárakban helyezkednek el, mint a Program Fájlok, vagy a Windows mappa. Az adminisztrátorok speciális intézkedések segítségével engedhetik csak ezt meg.
A Windows Szerver 2008 továbbá tartalmazza a Windows Resource Protection-t, amely segítséget nyújt a rendszerfájlok és registry bejegyzésekben keletkezett hibák kijavításában, amelyet szoftver-telepítések vagy más nem kívánt események idéztek elő.

3.13.1 EFS (Encrypting File System)

Az EFS az NTFS fájlrendszer részeként elég jelentős szerepet játszik a Castle Defense System-ben. Sokkal nagyobb biztonságot nyújt, mint a jogosultságok és engedélyek, mivel ha

egy illetéktelen személynek sikerül is fizikailag hozzáférni a titkosított fájlokhoz, azok tartalmát megtekinteni már nem lesz módja. Ez a módszer nem szükséges azon fájlok esetében, amelyek csak az NTFS engedélyeket tartalmazzák. Azonban az ideális biztonsági szint az, ha mind az NTFS engedélyeket, mind a titkosítást alkalmazzuk.
Ha azonban mixeljük az EFS-t a BitLocker-rel egy egészen magas védelmi rendszert kaphatunk. Azonban a legtöbb esetben, ha használjuk az EFS-t, az önmagában elegendő és nem szükséges a BitLocker használata. Ez főként olyan esetekben fordul elő, amikor érzékeny adatokat akarunk titkosítani, de az operációs rendszer teljes titkosítására ugyanakkor már nincs szükségünk. A titkosítást aktiválni ugyanott tudjuk, ahol a jogosultságokat is.
Azonban a titkosítást nem alkalmazhatjuk a tömörített fájlokon, mivel ez a 2 tulajdonság kölcsönösen kizárja egymást. Ezen kívül nem lehet titkosítani azokat a fájlokat sem, amelyek részei az operációs rendszernek, és azokat sem, amelyek a `%SYSTEMROOT%` mappában vannak. A WS2008 támogatja a megosztott mappában lévő fájlok titkosítását is, azonban amikor egy megosztott mappában lévő fájlt másol át valaki a hálózaton belül a saját számítógépére, az nem kell feltétlenül titkosítva legyen. Azonban amikor a kommunikáció megkívánja a teljes titkosítást, más technológiákat kell igénybe venni. Ilyenek lehetnek az IPSec (Internet Protocol Security) vagy az SSTP (Secure Socket Tunneling Protocol).
A WS2008 támogatja az offline fájlok titkosítását is, azonban a titkosított fájlok dekódolva lesznek abban az esetben, ha nem NTFS kötetre másoljuk őket. Ami még nagyon fontos, hogy a titkosítás nem védi a fájlokat a törléstől, mindössze védi a fájl tartalmát az illetéktelen személyektől. Így ha egyes felhasználóknak van joguk, arra hogy megtekintsék egyes mappák tartalmát, ezzel a titkosított fájlokat is (igaz azok tartalmát nem lesznek képesek látni), képesek lehetnek arra is, hogy kitöröljék őket. Ezért a titkosított fájlok zöld színnel jelennek meg a Windows Intézőben. A felhasználóknak ez segíthet a titkosított fájlok azonnali felismerésében. A fájl titkosítási folyamat egy egyszerű művelet, amely az alábbi lépésekből áll:

1. Nyissuk meg a Windows Intézőt.
2. Kattintsunk az egér jobb klikkjével a kívánt könyvtáron, majd válaszuk a Tulajdonságok párbeszédpanelt.
3. Az Általános fülön kattintsunk a Speciális gombra.
4. Válasszuk a *Tartalom titkosítása az adatbiztonság érdekében* opciót, majd nyomjunk OK-t.

5. Zárjuk be a Tulajdonságok párbeszédpanelt is.
6. Majd a felugró ablak megerősítésére is nyomjunk OK-t, miután bejelöltük a *Változások alkalmazása az alkönyvtárakra és fájlokra* opciót is.

Mostantól kezdve ezek a fájlok zölddel jelennek meg a Windows Intézőben. Az EFS használata, mint látjuk nem egy bonyolult dolog, azonban mint az informatika minden területén itt is vannak irányelvek, amelyeket érdemes követnünk és alkalmaznunk. Ezek a következők:

- Inkább könyvtárakat titkosítsunk, mint különálló fájlokat.
- Legyünk biztosak abban, hogy az offline fájlok titkosítva vannak.
- A teljes Dokumentumok mappa legyen titkosítva.
- Mind a %TEMP%, a %TMP%, mappák legyenek titkosítva, azért hogy az összes ideiglenes fájl szintén az legyen.
- Érdemes titkosítani a sorban-állási, úgynevezett spool- könyvtárat a nyomtató-szervernél.
- Érdemes társítani az EFS-t az IPSec-cel, vagy az SSTP-vel.
- Használjuk a csoport politikát (group policy) az EFS viselkedésének ellenőrzésére.
- Tudjuk biztonságban a visszaállító-ügynököt (recovery agent) és korlátozzuk az „ügynökök” számát a hálózatban.
- Használjuk a WS2008 nyilvános kulcsú infrastruktúráját (PKI- public key infrastructure) az EFS-hez és a visszaállító ügynökhöz.

Az EFS nyilvános és titkos kulcsokat használ a titkosítási és visszaállítási folyamatokhoz. A legjobb módszer, ha használjuk a Windows nyilvános kulcsú infrastruktúráját a kulcsok kezeléséhez. A dolgozat későbbi részében részletesebben foglakozom majd a nyilvános kulcsú infrastruktúrával (PKI).

3.14 A nyomtató rendszer biztonsága

A nyomtató rendszer biztonsága szintén fontos. Ahogyan korábban láthattuk, ha a fájlok titkosítva vannak a felhasználói rendszerekben, akkor titkosítva kellene legyenek a nyomtatási megosztott mappákban is. Azonban fontos ezt itt is megjegyeznünk, hogy mivel a felhasználóknak kezelési jogokat adtunk a nyomtatási mappához, amit valószínűleg azért

tettünk, mert megbízunk bennük. Használjuk az adatok kategorizálását ahhoz, hogy eldöntsük a nyomtató rendszer melyik mappája legyen védett, és titkosított.

3.15 A .NET keresztrendszer biztonság

A .NET keresztrendszer biztonsága egy másik megnyilvánulása az operációs rendszer megerősítésének. Először is a Windows Szerver 2008 központi elemként tartalmazza, mivel a keretrendszer 2-es verziója alapból installálva van, és a keretrendszer 3-as verziója is elérhető. Másodszor biztosítja a központi funkciókat a Web szolgáltatásokhoz. Ez biztosítja a 'motort' a működéshez és a végrehajtáshoz a Web szolgáltatásokat illetően. Ezen motor felelőssége, hogy meghatározza az adott kódról, hogy megbízható-e. Az összes kód egy ellenőrző folyamaton megy keresztül melynek neve közös futásidejű nyelv, azaz CLR (Common Language Runtime). A CLR 2 különböző módon alkalmazza a biztonságot, az első a 'kezelt kódokra' (managed code), a másik a 'nem kezelt kódokra' (unmanaged code) vonatkozik.
A kezelt kódú biztonság a CLR szívében van. A CLR 2 szempontból vizsgálja meg a kódot, mielőtt engedélyezi a futást: egyik a kód biztonságossága, a másik a kód viselkedése.
Az előnye ennek a fajta megközelítésnek a biztonságot illetően, az hogy nem kell a felhasználóknak azon aggódniuk, hogy a kód valóban biztonságos-e, azelőtt hogy futtatnák azt. Mivel ha biztonságos a CLR lefuttatja azt, ha nem biztonságos egyszerűen csak nem fut le. Azonban ez csak a kezelt kódokra vonatkozik.
A nem kezelt kódok esetében ez a fajta előny nem áll fent. Ahhoz hogy nem kezelt kódot futassunk, a CLR-nek engedélyek halmazát kell használnia, amelyek globálisan kell hogy deklarálva legyenek.

3.15.1 Kiértékelési folyamat kezelt kódok esetén

A CLR egy 10 lépésből álló kiértékelési folyamatot használ kezelt kódok esetén. A 10 lépés a következőkből tevődik össze (Lásd 3.15.1 ábra):

1. Amikor a kezelt kód egy része (assembly) meghív egy másik assembly-t, akkor a CLR kiértékeli a jogosultsági szintet, ahhoz hogy alkalmazza azt az új assembly esetén.
2. Az első dolog, amit az új assembly-nek tennie kell, hogy bizonyítékot szolgáltat. Ez a bizonyíték valójában, a CLR biztonsági politikájának kérdéseire adott válaszok halmaza.
3. A következő 3 kérdést kell megválaszolni az assembly eredetét illetően:

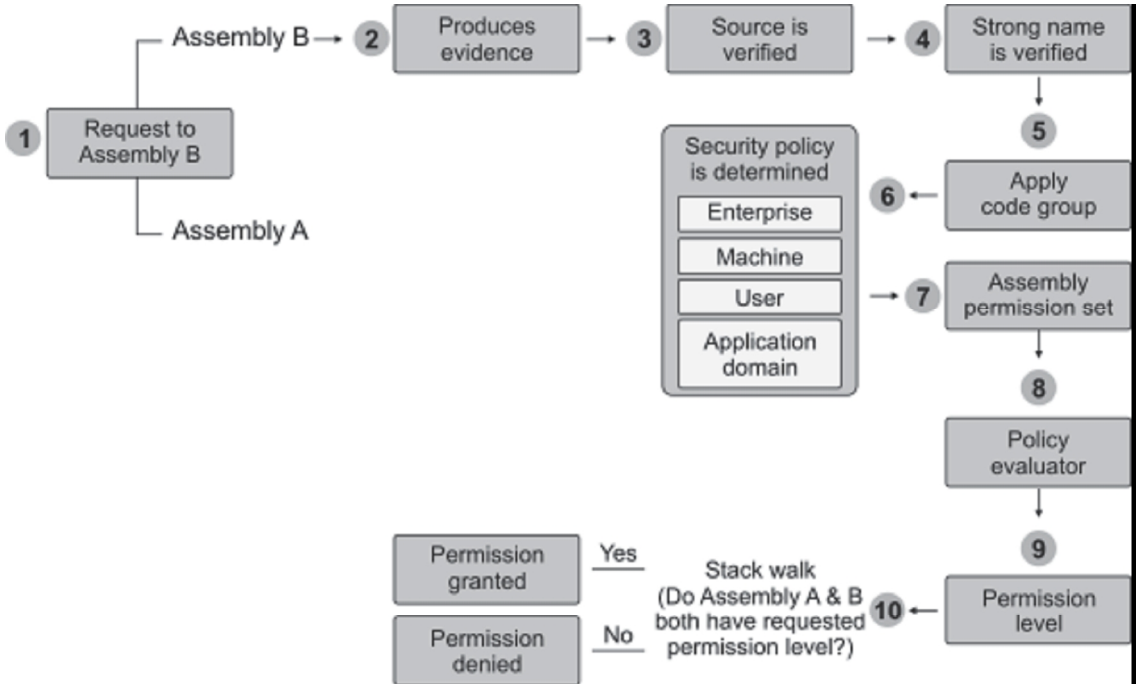
- Melyik web oldalról érkezett az assembly? Mivel az assembly-k automatikusan letöltődnek a kliensekre a web oldalról.
- Melyik URL (Uniform Resource Locator)-től származik az assembly? Az assembly-nek egy speciális URL címét kell szolgáltatnia.
- Melyik zónából érkezett az assembly? Ez vonatkozik az Internet Explorer zónákra, mint az Internet, Intranet, Helyi gép, stb. Néhány zóna sokkal megbízhatóbb, mint mások.

4. Az assembly-nek szintén szolgáltatnia kell egy kriptográfiailag erős azonosítót, egy úgynevezett ”erős nevet”. Ez az azonosító egyedi kell hogy legyen, és az assembly készítőjétől kell származnia. Nem kell feltétlenül azonosítania a szerzőt, de az assembly-t egyedien azonosítania kell.
5. A bizonyíték sok különböző forrásból ered, beleértve magát a CLR-t, a böngészőt, ASP.NET-et, a shellt, stb. Amint a bizonyíték adott, a CLR elkezdi maghatározni a biztonsági politikát, amit alkalmaznia kell. Előbb alkalmazza a bizonyítékot normál kód csoportokkal szemben, attól függően, hogy melyik zónából érkezett az assembly. A .NET keretrendszer alap kódcsoportokat tartalmaz, de az adminisztrátoroknak van lehetősége a sajátjait is hozzáadni.
6. Amint a kód csoport meg van határozva, a politika is adott lesz. Ezt a politikát 3 szinten kell érvényesíteni: Vállalat, Gép, Felhasználó szinten. A 4. szint magába foglalja az alkalmazás tartományát. Ez a tartomány egy izolált környezetet szolgáltat az alkalmazás futásához. Ez a környezet semmilyen más tartomány környezetéhez nem képes hozzáférni.
7. Amint a politika adott, egy kezdő jogosultsági halmaz keletkezik. Az assembly 3 módon tudja megszűrni ezt a halmazt:

- Először azonosítja azt a minimum halmazt, ami ahhoz kell, hogy az alkalmazás futhasson.
- Másodszor, meghatározhat opcionális engedélyeket. Ezek nem feltétlenül szükségesek.
- Harmadszor, egy „jól- viselkedő” assembly visszautasítja azokat az engedélyeket, jogosultságokat, amelyekre nincs szüksége, és túl kockázatosaknak látszanak.

8. Végül az összes tényezőt átnézi a kiértékelő. (policy evaluator)
9. A végleges jogosultságok beállítódnak az assembly-hez.

10. Az utolsó állomás a verem. A CLR összehasonlítja a jogosultsági halmazt az eredeti híváshoz tartozó más assembly-k jogosultságaival. Ha bármelyik assembly-nek nincs engedélye, hogy fusson ezzel a halmazzal, akkor a végrehajtás megtagadva. Ellenkező esetben a futás engedélyezve.



3.15.1 ábra A kiértékelési folyamat

3.16 Internet Information Services 7.0

Az IIS 7.0 azzal vált sokkal biztonságossá, mint elődje, hogy komponensekre bontották, így az egyes komponensek csak akkor telepítődnek, ha valóban szükségünk is van rájuk. Az egyik legbiztonságosabb tulajdonságát a Server Core-ban találjuk, mivel csak statikus weboldalakat szolgál ki. A korábbi biztonsági modellhez képest, ahol az ASP.NET és az IIS különálló entitásként volt jelen, az új modellben ezek együtt jelennek meg egy modellként.
Minden web oldalnak van egy alkalmazási tárolója, amely automatikus jön létre. Ez elkülöníti a weboldalt minden más oldaltól, vagy alkalmazástól a Web Szerveren. Ez az alkalmazási tároló a NetworkService alatt fut, és korlátozza a hozzáféréseket. Hogy biztosak legyünk abban hogy az alkalmazásunk ezen kontextus alatt fut, és csakis ez alatt, telepítenünk kell az Anonymous Authentication modult, és meg kell győződnünk arról, hogy az alkalmazás WEB.CONFIG fájlja tartalmazza a következő sort:

```
<anonymousAuthentication enabled="true" username=""
defaultLogonDomain="" />
```

Ez csak egyetlen példa volt az IIS megerősített biztonságáról. Ne feledjük, hogy a kulcspont a különálló komponensekben van. Mindig csak azt telepítsük, amelyikre valóban szükségünk van, és ezt követően támaszkodjunk a Biztonsági Konfigurációs Varázslóra.

4. réteg: Információ hozzáférés

A CDS 4. rétege a felhasználói azonosítással és felhasználók hálózaton belüli jogosultságaira tér ki. Akár csak a Windows 2003, a Windows 2008 is számos biztonsági protokollt tartalmaz az azonosításra és a hitelesítésre.

4.1 A Kerberos protokoll

Ezek közül az egyik legfontosabb főleg belső hálózatok számára a Kerberos, még akkor is, ha az NT LAN Manager (NTLM) továbbra is támogatott.
Habár a Kerberos protokollról mondanak jót és rosszat egyaránt, mégis sokkal több az előnye az NTLM –mel szemben. Gyorsabb, biztonságosabb, szélesebb körben elfogadott, és egyszerűbb a használata. Az egyik legjobb tulajdonsága pedig az, hogy ha egyszer a felhasználók hitelességéről meggyőződtünk, akkor a felhasználóknak nem kell újra és újra visszatérniük a szerverhez további engedélyekért. Míg ellenben az NTLM esetében, ahol a felhasználók folyamatosan visszatérnek a szerverhez jogosultság és engedély jóváhagyáshoz. A Kerberos esetében a felhasználók magukkal hordozzák az engedélyeket és a jogosultságokat a Kerberos szerver által biztosított hozzáférési jegyzékben, úgynevezett access token-ben. A szerver hitelesíti a klienst, és győződik meg arról, hogy engedélyezett a felhasználói hozzáférés a tartományon belül.
Végezetül a Kerberos szintén támogatja a 2-faktorú hitelesítést. Ez lehet akár smart kártya (smart card), biometrikus eszköz vagy ujjlenyomat vizsgáló berendezés is. Az egyik kulcseleme pedig az időbélyegzés. Az idő-szinkronizálás elengedhetetlen a Kerberosban, mivel a hitelesítő szerver összehasonlítja a saját belső óráját a kliens által feltett kérés idejével. Amennyiben az idő különbözet több mint a megengedett, akkor a szerver nem hitelesíti a felhasználót. Ez az egyik oka annak, hogy a Microsoft beintegrálta az időszolgáltatást az ADDS Emulator Operations Master szerepkörébe.

4.2 Smart Card hitelesítés

Az egyik legnagyobb előnye a smart kártyás hitelesítések használatának az adminisztrátori fiókok kapcsán jön elő. Mint korábban említettem a Windows 2008 támogatja a 2 faktorú hitelesítéseket. Ha magas biztonsági infrastruktúrát szeretnénk kialakítani, akkor mindenképpen ki kell használni ennek a hitelesítési lehetőségnek az előnyeit azon fiókok

számára, akik adminisztrátori jogkörrel bírnak. Sőt az adminisztrátoroknak érdemes 2 fiókot használnia, egy mezei felhasználó szintű fiókot a mindennapi tevékenységek végzéséhez, és egy adminisztrátori fiókot az adminisztratív tevékenység elvégzéséhez. Minden esetben normál felhasználóként kell bejelentkezniük, és az adminisztrátori tevékenységeket a 'Run as Administrator' parancson keresztül érdemes elvégezniük, használva a smart kártyát a jogosultság hitelesítéséhez. A smart kártyákról még lesz szó, ebben a fejezetben, mivel a kivitelezéshez szükségünk lesz egy nyilvános kulcsú infrastruktúrára (PKI).

4.3 Mi az SID?

A Windows hálózatok esetén, minden biztonsági entitást (security principal) egy egyedi számmal azonosítunk, melyet biztonsági ID-nak, vagy SID-nak hívunk. Minden felhasználó esetén a hozzáférési jegyzék (access token) tartalmazza az SID-kat. Az SID alapján dől el, hogy egy felhasználónak van-e hozzáférése egy adott objektumhoz vagy sem. A Windows 2008-ban minden biztonsági entitást egy szám azonosít, és nem egy név. Az objektumok birtoklása szintén ezen SID-kon alapul. Például amikor újra létrehozunk egy felhasználói fiókot, új SID-t jelölünk ki. Vagy amikor létrehozunk egy párhuzamos VSO (Virtual Service Offerings) hálózatot, és minden felhasználói fiókot áthelyezünk a régi tartományból az új tartományba, akkor minden felhasználónak új SID számot adunk. Azonban ilyen esetben a felhasználók a régi fájljaikhoz és mappáikhoz a régi SID alapján férhetnek hozzá, míg az áthelyezést követően, az új hálózatban a régi SID-kat le kell cserélnünk az újakra. Egy vándorlás folytán egy felhasználónak számos SID-ja lehet, melyet a felhasználók mind magukkal hordanak. Ezt hívjuk SID-history-nak, azaz SID nyomonkövetésnek.

4.4 Bizalom-kezelés a WS2008-ban

A Windows 2000 vezette be az automatikus két-irányú tranzitív bizalom (2-way transitiv trust) fogalmát egy Active Directory erdő (forest) esetén. A Windows 2008 kiterjesztette az erdők közötti tranzitív bizalom fogalmát az Active Directory Lightweight Directory Services megjelenésével. Habár ezen bizalmak többsége automatikus, továbbra is szükséges némi felügyelet. Számos bizalmi típus létezik a Windows 2008-ban, ezeket a következő táblázatban összesítem:

Bizalmi típusok (Types of trust)	**Irányuk és viselkedésük**	**Megjegyzés**
Szülő és germek	Két-irányú tranzitív	Automatikus bizalom, amely akkor épül fel, ha egy gyermek tartományt hozunk létre.
Fa-szerkezet (Tree-root)	Két-irányú tranzitív	Automatikus bizalom, amely akkor épül fel, ha egy új fát hozunk létre.
Erdő (Forest)	Egy vagy két-irányú tranzitív	Kiterjeszti a tranzitivitást 2 erdő között.
Rövidítés (Shortcut)	Egy vagy két-irányú tranzitív	Létrehoz egy rövidített utat a hitelesítéshez 2 tartomány között. A tartományok ezt az utat használják a hitelesítésre, ahelyett hogy végig haladnának a teljes hierarchia rendszeren.
Tartomány (Realm)	Egy vagy két-irányú tranzitív és nem tranzitív	Létrehoz egy hitelesítési linket egy Windows és egy nem-Windows (pl. UNIX) tartomány között.
Külső (External)	Egy vagy két-irányú nem tranzitív	Létrehoz egy hitelesítési linket egy Windows2008 tartomány és egy örökségi tartomány között.

4.5 Web Szerver hozzáférés ellenőrzés

Egy másik nagyon fontos terület, ahol a hitelesítés elengedhetetlen, az a web szerver. Az IIS számos különböző hitelesítési módokat kínál, amelyeket az alábbi táblázat tartalmazza:

MÓD	BIZTONSÁGI SZINT	KORLÁTOZÁS (HA VAN)	KLIENS TÁMOGATÁS	MEGJEGYZÉS
Anonymous	Nincs		Minden	Működik minden várható helyzetben
Alap (Basic)	Gyenge	Csak tiszta-szöveges jelszavak; csak SSL-nél használatos	Minden	Működik minden várható helyzetben
Kivonat (Digest)	Közepes		IE 5 vagy magasabb	Működik minden várható helyzetben
ASP.NET megszemélyesítés	Erős		Minden	NetworkService cserén alapszik
Windows Hitelesítés (Windows Authentication)	Erős		IE 5	Csak intranet esetben működik
Űrlap alapú hitelesítés	Nagyon erős		Minden	Belső alkalmazás hitelesítő metódusokon alapszik
ADDS kliens tanúsítvány-hitelesítés	Nagyon erős	A WS2008 támogatja az automatikus bejegyzéseket és frissítéseket a tanúsítványok esetén	Az összes újabb böngésző	Működik minden várható helyzetben

Általánosságban elmondható, hogy saját magunknak kell determinálni, hogy melyik hitelesítési mód a legjobb, és melyik passzol legjobban a web szerver követelményeihez. Figyelembe kell vennünk, hogy külső (external) vagy belső (internal) megoldásokról beszélünk, mivel teljesen más elveket követünk Internet esetében, és teljesen másokat egy belső hálózat esetében. A következő táblázat segíthet a döntésben. A hitelesítési mód az IIS konzolban van meghatározva, és alapbeállításként csak az ’Anonymous’ mód engedélyezett.

	Követelmények, kívánalmak	**Ajánlatok**
Intranet (Párhuzamos VSO hálózat)	- Minden kliensnek rendelkeznie kell egy Windows felhasználói fiókkal - Minden kliens legalább IE 6-ot használ - rendelkezünk egy magas színtű jelszótitkosítással	Használjuk a Kerberos protokollt a Windows Hitelesítésen keresztül
Internet	-Támogatnunk kell a különböző böngészőket és verziókat. -A legtöbb információnak a szerveren nyilvánosnak kell lennie. -Néhány adat és üzleti terv megkívánja a biztonságos belépést. - Nincs hatalmunk a felhasználók gépe felett, és nem akarunk tolakodók lenni sem. -Néhány szituációnak szüksége lehet delegálásra.	Ajánlott az Anonymous vagy az Alap SSL űrlapokkal
Extranet	-Ez nagyon biztonságos megoldást kíván. -Gyakran kölcsönös hitelesítést követel. -Gyakran 3. partnerre van szüksége, aki kezeli a kapcsolatot a szerver és a tanúsítvány tulajdonosa között. - A működés zökkenőmentes kell legyen.	Tanúsítvány-űrlapokkal

4.6 .NET keretrendszer hitelesítés

Mivel a .NET keretrendszer web szolgáltatásokat használ, így a hitelesítési modellek elég erősen az IIS-re támaszkodnak, igaz van néhány központi funkcionalitása a .NET keretrendszeren belül is. Ilyen például a szerepkör-alapú biztonság (role-based security, RBS). Az RBS 3 különböző típusú hitelesítésen alapszik: űrlap-alapuló hitelesítés (létrehoz egy sütit /cookie/), IIS hitelesítés, és Windows-hitelesítés. Az elsőt programozni kell, míg a második és a harmadik elvégezhető hálózati beállításokkal. A legegyszerűbb módja a felhasználók hitelesítésének és a hozzáférések engedélyezésének a belső hálózatban, ha szerepköröket

határozunk meg. A szerepkörök nem mások, mint csoportosítások a különböző hozzáférési szintek esetében az egyes alkalmazások tekintetében. Ezek a csoportosítások alkalmazás-függők, de feltérképezhetők az ADDS-ben. A hozzáférések engedélyezését a szerepkörök hozzárendelése előtt kell megtennünk. Ezt az Authorization Manager-en keresztül végezhetjük el, az AZMAN. MSC parancs futtatásával. A fejlesztőknek létre kell hozni egy kezdeti listát, majd ezt hozzácsatolni az alkalmazáshoz, majd az adminisztrátorok rendelik hozzá ehhez a felhasználókat és a csoportokat. Ez a biztonsági modell egy nagyon hatásos modell, és kevesebb irányítást igényel, mint a korábbi alkalmazás-hitelesítő sémák.

4.7 Ellenőrzés és megfigyelés

Nagyon fontos, hogy nyomon kövessük az erőforrás használatokat és naplózzuk a fájl hozzáféréseket, hogy megbizonyosodjunk arról, hogy a felhasználók a megfelelő jogokkal rendelkeznek, és senki sem próbálta meg ezeket a jogokat felülírni vagy megváltoztatni. Ahogyan azt korábban említettük, az auditálás egy két-lépéses folyamat. Előbb engedélyeznünk kell az auditálást egy esemény számára. Majd ezt az auditálást be kell kapcsolnunk a megfelelő eseményre, és azonosítanunk kell a személyt, akire szeretnénk a nyomon követést végrehajtani. A Windows 2008 számos esemény típusra engedélyezi az auditálást. Ezek közül a legfontosabbak:

- felhasználói bejelentkezések
- objektumokhoz való hozzáférések
- rendszer események
- folyamatok nyomon követése
- politikák megváltoztatása

Az auditált objektumok és események lassítják a rendszert, ezért nagyon fontos, hogy csak azokat ellenőrizzük, amelyeket kritikusnak vélünk. Ellenőrizhetjük egy esemény sikeres megtörténtét vagy sikertelenségét is. Azonban csak akkor auditáljuk az események sikertelenségét, ha illetéktelen tevékenységekre gyanakszunk a hálózaton belül. Ez csökkentheti az auditált események számát, így kevésbé lassíthatjuk a rendszerünket.

5. réteg - Külső hozzáférések

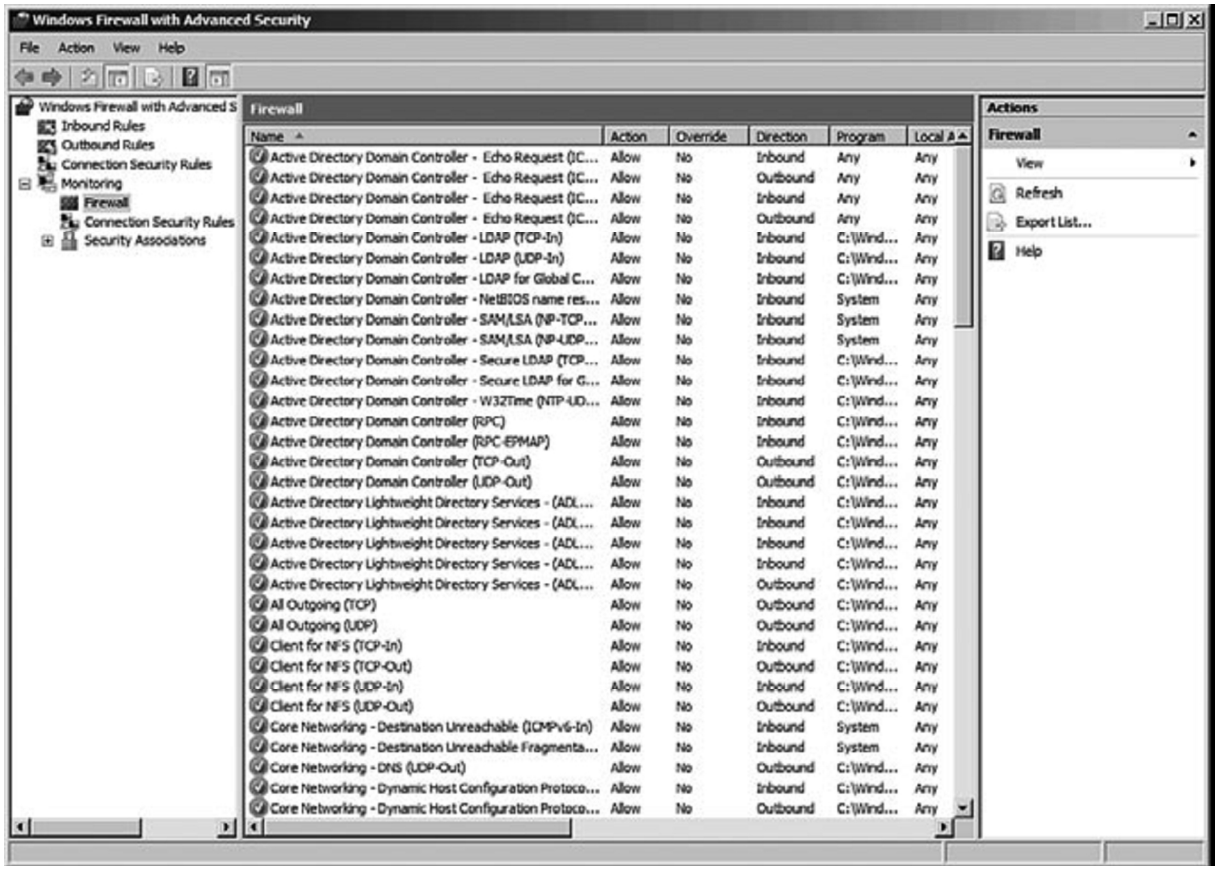
A CDS (Castle Defense System) 5. rétege a külső hatásokkal szembeni védekezésre összpontosít. A mai összekapcsolt világunkban eléggé lehetetlen olyan hálózatot létrehoznunk, amely 100%-ig védve van a külső világunk hatásaival szemben. Ezért is kell a lehető legjobban megvédenünk a belső hálózatot, és gátakat, korlátokat felállítanunk mielőtt a külvilággal bármilyen kapcsolatot hoznánk létre. Ezek a gátak és korlátok számos formában megjelenhetnek. Ezt a körülvevő környezetet hívjuk demilitarizációs zónának, vagy DMZ-nek.

5.1 Windows Szerver Tűzfal kibővített biztonsággal

Az egyik legfontosabb eszköz, amelyet használnunk kell, nem más, mint az új Windows Szerver Tűzfal Kibővített Biztonsággal (Windows Server Firewall with Advanced Security, WSFAS, lásd 5.1 ábra). A Windows Tűzfal mára már minden Windows operációs rendszer szerves része, és alapbeállításként telepítve van, és úgy van beállítva, hogy alapbeállításként minden távoli kapcsolatot elutasít. Majd miután kialakítottuk a szerverünk szerepkörét, lehetőségünk van arra, hogy módosítsuk a tűzfal beállításait, és portokat nyissunk meg a kapcsolatok számára. A legfontosabb különbség a régi tűzfalak, és az új WSFAS tűzfal között, hogy az utóbbi kombinálja a tűzfal adottságait az IPSec-kel, így egyetlen közös eszközt létrehozva, amely nem csak a bejövő és kimenő kapcsolatokat felügyeli, de figyeli a virtuális magánhálózatok forgalmát is. Az IPSec (Internet Protokoll security) Internet szabványok halmaza, amely kriptográfiai védelmet nyújt az IP forgalom számára. A Winodws XP és Windows Szerver 2003-ban a Tűzfal és az IPSec külön-külön jelent meg. Azonban mivel mindkettő a bejövő és kimenő forgalmat szűrte meg, így ezt a kettőt összehangolták. Kivételeket adhatunk meg, amelyekkel explicit szűrhetjük a bejövő és kimenő forgalmat. TCP (Transmission Control Protocol) és UDP (User Datagramm Protocol) portokat tilthatunk le, mind forrás és mind cél tekintetében, illetve ICMP (Internet Control Message Protocol) és ICMPv6 (ICMP for IPv6) forgalmat típus és kód szerint is szűrhetünk.

Sok mindent lehetne még mondani a tűzfalról, de általánosságban elmondható, hogy támaszkodjunk a lehető legjobban a Biztonsági Konfigurációs Varázslóra, amely segít a tűzfal teljes konfigurálásában.

Azonban tartsuk szem előtt, hogy maga a tűzfal önmagában nem elegendő.



5.1 ábra Windows Firewall with Advanced Security

5.2 SSTP (Secure Sockets Tunneling Protocol)

Hagyományosan a VPN (Virtual Private Network) kapcsolatok az IPSec protokollra támaszkodnak, amely támogatja az ’end-to-end ’ kapcsolatokat a hálózati rétegben. Azonban ezek a magán hálózati kapcsolatok nem működnek minden szituációban. Például web proxy szerverek esetében, amikor a kapcsolat már a ’kapunál’ blokkolva lesz.

Ez az egyik oka annak, hogy a Microsoft megvalósította az SSTP protokollt. Az SSTP a HTTPS-re (Hyper Text Transfer Protocol over Secure Socket Layer) támaszkodik, és hoz létre VPN kapcsolatot a 443-as porton. Támogatja a NAP-ot (Network Access Protection) és IPv6-ot is. Amikor létrehozunk egy ilyen magánhálózatot, akkor a kliens gép kialakít egy egyedülálló kapcsolatot a belső szerverrel, és minden egyes forgalom ezen a kapcsolaton keresztül valósul meg. Nem áll módunkban használni ezt a kapcsolatot ’site-to-site’ kapcsolat létrehozására. Az SSTP nyilvános kulcsú infrastruktúrára (PKI) támaszkodik a kapcsolat létrehozásához. Ezt a PKI-t vizsgáljuk meg egy kicsit a következő részben.

5.3 PKI (Public Key Infrastructure)

A PKI implementációk elég komplexek lehetnek, főleg akkor, ha kliensek és a belső hálózaton kívüli ellátók közötti intermezzóra használjuk őket. Ebben az esetben a legfőbb dolog a bizalom: Valóban az valaki, akinek mondja magát és bízhatunk-e a tanúsítványaiban? Ilyen esetekben egy harmadik fél szaktekintélyére kell támaszkodnunk, aki kezeskedik arról, hogy valóban az valaki, akinek mondja magát. A Windows 2008 jelentős szerepet játszhat abban, hogy lecsökkentse ezen infrastruktúra költségeit. Mivel tartalmazza az összes szükséges tulajdonságot, ahhoz hogy létrehozzunk egy PKI szolgáltatást az ADCS (Active Directory Certificate Services) szolgáltatáson keresztül, csupán annyit kell tennünk, hogy meg kell szereznünk a gyökér szerver tanúsítványt (root server certificate) egy külső forrásból, majd ezt a tanúsítványt fogjuk beágyazni minden egyes tanúsítványba, amelyet mi adunk ki. Ez bizonyítani fogja a partnerek és kliensek számára, hogy valóban azok vagyunk, akiknek mondjuk magunkat. Így nem kell megvalósítanunk egy drága harmadik személyt igénylő PKI megoldást.

Azonban nincs szükségünk erre a típusú tanúsítványra a belső hálózat esetén, mivel mi magunk irányítjuk az összes rendszert a hálózatban, és nem kell bizonyítanunk, hogy valóban mi vagyunk azok. Az ADCS számos biztonsági helyzet típust támogat:

- használhatjuk web szolgáltatások, szerverek, alkalmazások biztosítására
- elektronikus levelek digitális aláírására
- kódok aláírására
- támogatja az EFS-t
- támogatja a smart kártyás bejelentkezést
- a virtuális magán hálózatokat
- a távoli elérés hitelesítést
- a vezeték nélküli hitelesítést

A Windows Szerver 2008 két típusú tanúsítvány-hatóságot (certificate authority, CA) biztosít: egyedülállót (stand-alone) és vállalatit (enterprise). Az utóbbi teljes integritást biztosít az ADDS-sel (Active Directory Domain Services). Az enterprise CA előnye hogy biztosítja az automatikus bejegyzést és automatikus meghosszabbítást.

5.4 NAP (Network Access Protection)

Egy másik nagyon hasznos funkciója a Windows Szerver 2008-nak a NAP (Network Access Protection). A külvilággal való kapcsolat létesítése előtt a kliensnek bizonyos feltételeknek eleget kell tenniük. Ami azt jelenti, hogy azok a kliensek, amelyek ezeket nem teljesítik - mint például nem rendelkeznek napra-kész frissítésekkel, vírusirtó rendszerekkel, szerviz csomagokkal – akkor elszigetelté válnak, és egészen addig, amíg ezt nem bizonyítják, nem létesíthetnek kapcsolatot a külvilággal. A Windows Vista óta tartalmazzák ezt a fajta védelmet az operációs rendszerek alapbeállításként.

A NAP karantént vagy korlátozott hozzáférést kényszerít ki a következő technológiáknak:

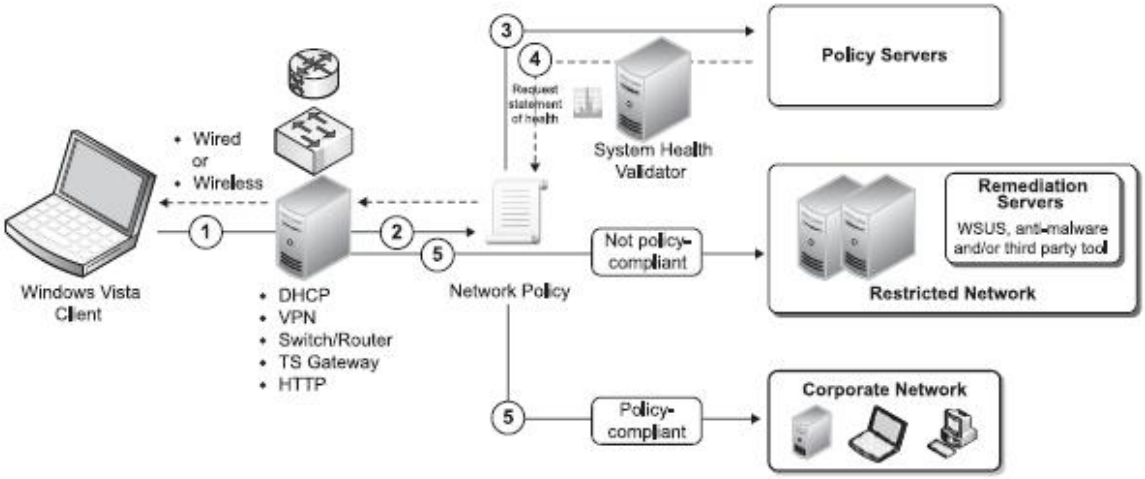
- IPSec kapcsolatoknak
- Vezetékes (IEEE 802.3) kapcsolatoknak
- Vezeték nélküli (IEEE 802.11) kapcsolatoknak
- DHCP kapcsolatoknak
- Virtuális magán hálózatoknak
- HTTP-n alapuló HCAP kapcsolatoknak (Host Credential Authorization Protocol)
-

A NAP kapcsán beszélhetünk a kliensek ’egészségi ’ állapotáról. (health status) illetve ezen állapot meglétét jóváhagyó úgynevezett ’egészségi állapotot jóváhagyó szerverről.’ (Health Validation Server). A NAP erre a szerverre támaszkodik ahhoz, hogy megállapítsa a kliensek egészségi státuszát.

Minden kapcsolat esetében létezik egy kérés (request), aminek az NPS-en (Network Policy Server) keresztül kell mennie, és a következőképpen kell működnie:

1. A kliens egy kérést kezdeményez a vezetékes vagy vezeték nélküli kapcsolatot használva.
2. A kapcsolat ellátó (HTTP, DHCP, VPN, Router, Switch) ellenőrzi a hálózati politikát (network policy), hogy mit is kezdjen a kéréssel.
3. A szerver (Network Policy Server) átadja az ellátónak a szükséges és helyes politikát.
4. Az ’egészségi állapotot jóváhagyó szerver’ (Health Validation Server) megállapítja a kliens egészségi állapotát, és ezt visszaküldi az ellátónak (provider).
5. A kliens egészségi állapotától függően 2 dolog történhet:

- Ha a kliens nem tűnik kellően ’egészségesnek’, akkor korlátozott hálózatba kerül. A korlátozott hálózat karanténba helyezi a rendszert, amíg a szükséges állapot be nem következik. A korlátozott hálózat csak a Windows Server Update szolgáltatásaihoz enged hozzáférést, illetve a napra-kész állapot eléréséhez szükséges eszközökhöz. Amint a kliens frissítve lesz, az egészségi állapota szintén frissítésre kerül, így ha az új egészségi státusz megfelelő az ellátó teljes hozzáférést enged a külvilághoz.
- Ha a kliens ’egészségesnek’ látszik, akkor teljes hozzáférést kap a külvilághoz.



5.4 ábra Network Access Protection

Összefoglalás

A dolgozat írásakor célom a legfrissebb Microsoft operációs rendszer, a Windows Szerver 2008 biztonsági szempontból történő átvizsgálása volt. Az elkészítést nehezítette, hogy a témában semmilyen magyar nyelvű szakirodalom nem állt a rendelkezésemre, így csakis a témavezetőm angol nyelvű elektronikus könyveire és az Internet adottságaira támaszkodhattam. Az angol nyelvű szakirodalom pedig elég szerteágazó volt.

Megpróbáltam érthető és világos lenni a megfogalmazásokban, de sokszor az eredeti angol kifejezéseket zárójelben meghagytam, hogy még véletlenül se legyek félreérthető. A dolgozat tartalmi megkötöttsége miatt próbáltam nem elveszni a részletekben, de ugyanakkor minden fontosabb biztonsági elemet érinteni. Mivel én magam is a Windows operációs rendszerek mellett teszem le a voksom, így fontosnak éreztem, hogy biztonsági szempontból megvizsgáljam az operációs rendszerek legújabb példányát.

Hogy biztonsági szempontból mit hoz a jövő, arra a Microsoft operációs rendszerek következő generációjának képviselője adja majd meg a választ, amely jelenleg a **Windows 7** (Windows Seven) kódnevet viseli. Sajtóértesülések szerint még fejlesztés alatt áll, és előreláthatólag 2010-ben látja meg a napvilágot.

Hogy mit várhatunk nagyvonalakban a Microsoft operációs rendszereitől a jövőben?

- A webes és helyi adattárolás, keresés várhatóan egyre közelebb kerül egymáshoz, egységes platform alatt végezhetjük el a különböző műveleteket dokumentumainkkal, legyenek azok a helyi gépen, a hálózaton, esetleg a világhálón.
- Nagyobb biztonság. Az adattárolásnál jelenleg használt titkosítási eljárások a perifériákra is kiterjednek majd. A **Windows** 7 támogatni fogja az úgynevezett szerepkör-függő konfigurálást, valamint a korábbinál szigorúbb, de könnyebben menedzselhető felhasználó kezelést.
- A **Windows** 7 tovább növeli a mobil számítógépek hatékonyságát. A vezeték nélküli kapcsolatok funkcionalitása és biztonsága tovább nő, valamint lehetővé válik a kvázi eszközfüggetlen mobilszinkronizáció. Az új rendszer flexibilisen lesz képes alkalmazkodni a robusztus óriáshálózatok és a néhány gépes otthoni hálózatok környezetéhez.

- A **Windows** 7 az alkalmazások könnyebb migrációjával olcsóbb megoldást kínál majd a vállalatoknak. Miközben továbbra is teljesen kompatibilis marad a korábbi verziókkal, kiszámíthatóbb áttérést és fejlesztést tesz lehetővé.

Köszönetnyilvánítás

Ezúton is köszönetet szeretnénk mondani Dr. Krausz Tamás egyetemi adjunktusnak a diplomamunka elkészítéséhez nyújtott segítségéért.

Irodalomjegyzék

Danielle & Nelson Ruest –
Microsoft Windows Server 2008, The Complete Reference, 2008 – eBook

Rand Morimoto, Michael Noel, Omar Droubi, Ross Mistry, Chris Amaris –
Windows Server 2008, Unleashed, 2008 – eBook

Jeffrey R. Shapiro –
Windows Server 2008, Bible – eBook

http://www.microsoft.com/technet/security/prodtech/windowsserver2008/default.mspx
http://www.microsoft.com/whdc/system/platform/hwsecurity/default.mspx
http://www.technet.microsoft.com/en-us/library/cc700820.aspx
http://www.symantec.com/enterprise/products/category.jsp?pcid=2241
http://www.microsoft.com/technet/network/nap/default.mspx.
http://redmondmag.com/techlibrary/resources.asp?id=101
http://www.microsoft.com/technet/network/wf/default.mspx
http://winportal.net/?id=1058