

SZAKDOLGOZAT

Makleit Nándor

Debrecen

2009

Debreceni Egyetem
Informatika Kar

Biztonság MS Platformon

Témavezető:
Dr. Krausz Tamás
Egyetemi adjunktus

Készítette:
Makleit Nándor
Programtervező Informatikus

Debrecen
2009

Tartalomjegyzék

Bevezetés	1
A Windows Vista és Windows Server 2008 védelme	3
Autentikációs tár	7
Autentikációs protokollok	10
Személyes értékek	11
Felhasználói fiók felügyelet (UAC)	12
Tűzfal	15
A Windows tűzfal javításai	16
IPsec	19
Network Access Protection	21
Szolgáltatások	24
Támadások szolgáltatások ellen	25
Csoportházirend	31
Összefoglalás	33
Irodalomjegyzék	33

Bevezetés

Miből ne venné ki manapság az informatika a maga részét? A szervezetek működésében elengedhetetlen az információ technológia jelenléte. Más gépekkel ellentétben itt nem csak a meghibásodások okoznak problémát. Ellenfeleink próbálnak meg betörni a hálózatunkba, belépni a szerverünkre, ledönteni azt, vírusokkal megfertőzni vagy információt szerezni a vásárlóinkról, alkalmazottainkról. A támadások szinte minden irányból jönnek: belső emberektől kezdve, fertőzött weboldalakon keresztül külső, Virtual Private Network-ön (VPN) keresztül kapcsolódó emberekig, a hálózatban levő sebezhető gépeket vagy szervereket érő közvetlen támadásokon át. Ma már a szervezeteknek mérettől függetlenül kell egyre komplexebb átvizsgálási követelményekkel szembenéznük.

Tudhatjuk, hogy mennyire lényegesek a szerverek a cégek helyes működésében és feltörekvésében. Az adatok, amiket tárolnak, a szolgáltatások amelyeket nyújtanak, az életet adó vért jelentik a cég ereiben. Az pedig a mi feladatunk, hogy őrt álljunk a birtokunk körül, megvédve a külső vagy belső támadásoktól, az összeomlástól, és biztosítsuk az ellenőrzésen, hogy mi minden indokolt lépést megtettünk a szerverünk védelme érdekében.

A Microsoft Windows Server 2008 tervezésekor végig a biztonság volt a középpontban, egy sor új, valamint továbbfejlesztett technológia felhasználásával, amelyek így kialakították a szilárd alapjait, segítve ezzel minket az üzleti életben.

A Microsoft Windows Server 2008 a Windows Server operációs rendszer következő generációját képviseli. Maximális irányítási lehetőséget nyújt az informatikusoknak az infrastruktúra fölött, ugyanakkor folyamatos rendelkezésre állást és felügyeleti lehetőségeket kínál. Ez minden eddiginél biztonságosabb, megbízhatóbb és robusztusabb kiszolgáló-környezetet eredményez. A Windows Server 2008 új előnye a szervezetek számára, hogy helytől függetlenül minden felhasználónak garantálja a hálózat minden szolgáltatásának elérését. A Windows Server 2008 ezenkívül részletes és alapos információkkal szolgál az operációs rendszerről, diagnosztikai lehetőségeket tartalmaz.

A Windows Server 2008 a díjnyertes Windows Server 2003 operációs rendszer sikerére és erősségeire, valamint a Service Pack 1 csomagban és a Windows Server 2003 R2 kiadásban

foglalt újdonságokra épül. A Windows Server 2008 azonban sokkal több, mint pusztán a korábbi operációs rendszerek csiszoltabb változata. A Windows Server 2008 a leghatékonyabb platform az alkalmazások, hálózatok és webszolgáltatások számára a munkacsoportoktól kezdve egészen az adatközpontokig; érdekes és értékes új és tökéletesített funkciókkal egészíti ki az alap operációs rendszert.

2008. február 27-én jelent meg, csaknem 5 évvel elődje, a Windows Server 2003 után. Fejlesztése során 2007. május 16-áig Longhorn kódnéven volt ismeretes, míg a Microsoft akkori elnöke, Bill Gates bejelentette hivatalos nevét, a Windows Server 2008-at a WinHEC konferencián. Magyarországon a termékbejelentésre 2008 március 5-én került sor, a Lurdy-házban.

A Windows Server 2008 kódbázisa a Vistáéval megegyezik, ezért architektúrájukban és funkcionalitásukban is sok közös vonás található. A közös kódbázis miatt a Windows Server 2008 automatikusan tartalmazza a Vista technológiai, biztonsági és menedzsment terén hozott újdonságait, mint például az újraírt hálózati protokollverem (networking stack), benne natív IPv6, natív vezeték nélküli hálózat, sebességi és biztonsági fejlesztések; továbbfejlesztett lemezkép-alapú telepítés, kiszolgáló-konfigurálás és visszaállítás; továbbfejlesztett diagnosztikai, rendszerfelügyeleti, eseménynaplózási és jelentéskészítő eszközök; új biztonsági funkciók, mint a Bitlocker és az ASLR (véletlenszerű címterület-kiosztás); továbbfejlesztett Windows tűzfal biztonságos alapértelmezett beállításokkal; .NET Framework 3.0 technológiák, mint a Windows Communication Foundation, Microsoft Message Queuing és a Windows Workflow Foundation; továbbá alacsony szintű kernel-, memóriakezelési és fájlkezelési fejlesztések. A processzor- és memóriaeszközök kezelését a Plug and Play eszközök mintájára oldották meg, alkalmas hardveren lehetővé téve ezek menet közbeni cseréjét (hot-plugging). Szintén lehetővé vált a rendszer erőforrásainak dinamikus felosztása, azaz a Dynamic Hardware Partitioning; minden hardverpartícióhoz saját memória-, processzor- és I/O host bridge eszközök tartoznak, amik függetlenül vannak a többi hardverpartíció eszközeitől

A Windows Vista és Windows Server 2008 védelme

A biztonság egyik legalapabb szintjén a tényezőket két fő kategóriába sűrítjük: Tárgyak, amelyeket megvédünk, és dolgok amelyektől megvédjük. Ezek használatára kerül a sor, hogyha autentikálunk (ellenőrizzük, hogy kik vagyunk), felhatalmazunk (belépési jogot adunk valamire) vagy ha ellenőrzünk valamit (végigkövetjük, ki hova lépett be). Maguk a fogalmak alapvetően nagyon egyszerűek. A tárgyak, melyeket védünk, a fájljaink. Akik ellen védeni kell, a felhasználók. Az autentikáció (authentication), felhatalmazás (authorization) és az ellenőrzés (auditing) ezen fájlok és felhasználók kölcsönhatását vizsgálják. Azaz ilyen módon folytak régebben az események; de egyes egyszerűbb rendszerekben még ma is ilyen eszközök állnak rendelkezésre. Akárhogy is, a Windows, ha a biztonságról van szó, mérhetetlen gazdag eszközzel rendelkezik. A felhasználók nem egyszerű felhasználóként jelennek meg, máshogy történik a besorolásuk. Elég gyakran találkozhatunk biztonsági meghatalmazásokkal. A Windows szóhasználatában ezek nem feltétlen egy-egy konkrét embert jelölnek, hanem akár csoportokat vagy számítógépeket. Ezek a meghatalmazások akármi lehetnek, amik kapcsolatba hozhatóak a SID-del (biztonsági azonosító) vagy jogot adnak valahova történő belépésre.

Felhasználók:

Egyszerűen csak egymástól különböző egyedek, amik bejelentkeznek a számítógépen. Alapjában véve ezek valamilyen módon kapcsolatba hozhatóak a biztonsági meghatalmazásokkal.

A felhasználóknak két csoportja van: helyi(local) és tartományi(domain). A helyi felhasználók a lokális SAM-ban kerülnek leírásra (Security Accounts Manager). Minden Windows-alapú számítógép rendelkezik SAM-mel, ami tartalmazza az adott gép felhasználóit.

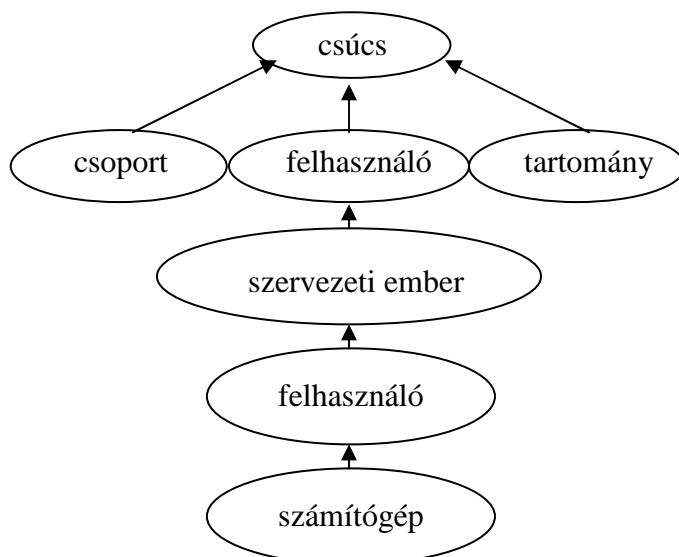
Rendszerint úgy hiszik, hogy a tartományvezérlőknek (Domain Controller, DC) nincs helyi SAM-ük, mivel nem helyi felhasználók. Ez nem igaz. A tartományvezérlőkhöz is tartozik helyi SAM. Alaphelyzetben két féle felhasználó létezik: Adminisztrátor és Vendég. A vendég le van tiltva alap beállítások mellett.

A Windows Server 2008-ban az alap engedélyezett felhasználó az adminisztrátor. (Kivéve egy Cougar kódnevű Windows szerver, egy kisebb, üzleti szerver verziója a Server 2008-nak, hivatalos nevet nem jelentettek be.) Első bejelentkezés az adminisztrátorral történik. Windows Vista alatt az adminisztrátor le van tiltva és csak nagyon korlátozott körülmények között tudjuk használni. Mindkét esetben erősen javallott új felhasználókat bejegyeztetni minden egyes embernek, akik irányítják a megadott gépet. (Hogyha követjük az előírásokat, ez szabály, Libenson, 2006.) Egy felhasználó egy ember saját, személyes tulajdona. Hogyha az adminisztrátoroknak nem igazgatással, irányítással kapcsolatos dolgot kell ellátniuk, szükségük lesz egy nem adminisztrátor felhasználói fiókra.

A másik fajta felhasználói fiók a tartományi felhasználó. A tartomány a DC-ben kerül leírásra, és bárholnan lehet használni a tartományom belülről. A tartományi fiókoknak jelentősen több tulajdonságaik lehetnek a helyiekhez képest. Bővebb szemantika több tulajdonságba burkolva, szervezeti környezetben, például telefonszámok, e-mail címek, stb. A tartományi felhasználói fiókok sokkal hasznosabbak a hálózatban, mivel más számítógépeken keresztül lehet használni. Tartományban történő felhasználó létrehozás megkönnyíti a kezelést is.

Számítógépek:

Valójában a számítógépek csak egyfajta felhasználók. Az Active Directory-ban ez különösen igaz, ahogyan az öröklődési modell is alátámasztja.



Öröklődési hierarchia, a számítógépek és felhasználók kapcsolatáról.

Néhány érdekességet észrevehetünk az ábrából. Legelőször, ahogyan azt láthatjuk is, az Active Directory minden osztálya a csúcsból ered. Valójában a csúcs is a csúcs alosztályaként van számon tartva. Másodszor, a felhasználó a szervezeti ember osztályból ered. Harmadszor –és ez a legérdekesebb része a dolgoknak- a számítógépet a felhasználóból származtatják. Más szavakkal, az objektum-orientált kifejezés az lenne, hogy a számítógép egyfajta felhasználó. Az, hogy a számítógépeket ennyire emberinek kezeljük, nagyon sok értelmet nyer, ha be tudjuk látni, hogy muszáj emberekként kezelni azokat, mivel gyakorlatilag ugyanazok a jellemzőik.

Csoportok:

Ne feledjük, vannak fájljaink, amelyeket el szeretnének érni. Az operációs rendszer hagyja jóvá ezt az elérési kísérletet azzal, hogy ellenőrzi a jogainkat. Nagyon régen, a kezdetek kezdetén az operációs rendszert tervező emberek felismerték, hogy nagyon kezelhetetlenné válna a helyzet, ha minden egyes fájlhoz jogokat rendelnénk minden felhasználó számára, akinek szüksége van az elérésére. A probléma megoldására létrejöttek a csoportok, amik tagjai a felhasználók lettek. Ez feljogosít arra, hogy jogokat rendeljünk a csoportokhoz, a felhasználókon túl. A csoport nem lehet egy felhasználó, de még mindig egy biztonsági meghatalmazás, azonosítóval, mint a felhasználók és számítógépek. A Windowsban egy felhasználó sok csoport tagja lehet, és a dolgaink sok csoporthoz kapcsolnak jogokat. Egymásba illesztett csoportoknak is vannak jogaik, némi korlátozással. Egy nem-tartományból származó irányítónak csak két fajta csoportja lehet: beépítettek és a helyiek, amiket az adminisztrátor definiál. Azonban az Active Directory-ban hat fajta csoporttal találkozunk: beépített tartomány helyi-, globális-, univerzális csoportok; valamint a felhasználó által definiált tartomány helyi-, globális- és univerzális csoport. Tartomány helyi csoportjainak csak erőforrásokra oszthatnak ki jogokat, de azok tartalmazhatnak felhasználókat, univerzális- és globális csoportokat bármilyen megbízható tartományból vagy erdőtől, mint ahogy a tartomány helyi csoportjai a saját tartományukból. Egy globális csoport csak felhasználókat és globális csoportokat tartalmazhat a tartományból, ahol definiálták, de hozzá tartozhat jog bármilyen erdőbeli tartományból, aminek tagja, vagy megbízható erdőből. Az univerzális csoportok felhasználókat, univerzális- és globális csoportokat bármilyen tartományból tartalmazhatnak. Egy univerzális csoportnak bármelyik megbízható tartomány vagy erdő erőforrásaihoz lehetnek jogai.

Szolgáltatások

Az állandó vita a host alapú tűzfalokról éveken át tartott. Rengeteg ember, főleg a termékeiket eladók azon vitatkoztak, hogy a host alapú tűzfalnak a kimenő forgalmat is meg kellene szűrnie ahhoz, hogy érjenek is valamit, mert azzal védik a hálózatot egy veszélyt jelentő számítógéptől. Objektíven rámutattak, hogy ha egy számítógép veszélyt jelent, a rosszindulatú szoftver már jelen van, és képes arra, hogy túljusson vagy kikapcsolja a host alapú tűzfalat teljesen. Természetesen, ha a veszélyt jelentő szoftver egy alacsonyabb jogokkal rendelkező alkalmazáson keresztül jutott fel a gépre, ez az érv nem helyénvaló. Az elmúlt években a Microsoft jelentős időt töltött el azzal, hogy alacsonyabb jogokkal futó alkalmazásokat indítson, de egy szolgáltatás más szolgáltatásokat is irányít, amit az adott felhasználó futtat, és bármit megtehet, amit egy szolgáltatás. Éppen ezért, ha szolgáltatás_A forgalmat bonyolít a tűzfalon keresztül, de szolgáltatás_B nem tud, szolgáltatás_B átveheti szolgáltatás_A-t mindaddig, amíg azonos felhasználó alatt futnak. Hogy kezelhető legyen ez a probléma, a Microsoftnak szüksége volt egy megoldásra, hogy jogokat társítson a folyamatokhoz, vagy még speciálisabban, a szolgáltatásokhoz. Minden szolgáltatásnak van egy azonosítója, ami arra való, hogy jogokat párosítsunk hozzá. Azzal, hogy megjelöljük, mely jogokat tiltunk egy azonosítóhoz, biztosítjuk, hogy a biztonsági meghatalmazások be legyenek nyújtva egy kérelem indításakor, figyelmen kívül hagyva, hogy miféle más jogok tartoznak ahhoz a dologhoz. Hirtelen értelmet nyert, hogy kimenő, host alapú tűzfalak szűrőjét használjuk egyes helyzetekben, úgyhogy a tűzfalak a Windows Vistában és Windows Server 2008-ban már támogatják azokat. Alaphelyzetben blokkolja a szolgáltatások kifelé menő forgalmát, kivéve, ha azokon a portokon megy, amire amúgy is szüksége van a szolgáltatásoknak. Ez egyenesen akkora biztonság, amekkorát csak elvárhatunk a host alapú tűzfalaktól.

Biztonsági azonosítók (Security Identifiers)

Korábban már említésre került, hogy a biztonsági meghatalmazások azok önálló egyedek, melyeknek lehetnek biztonsági azonosítójuk (SID-jük), a SID-ről viszont még nem volt szó. A SID általában véve a meghatalmazás numerikus reprezentációja. A SID tulajdonképpen az, amit az operációs rendszer belül használ. Amikor egy felhasználóhoz, csoporthoz, szolgáltatáshoz vagy bármi máshoz biztonsági jogokat adunk, az operációs rendszer beírja a jogot a hozzáférési listájába. (Access Control List, ACL).

Összesítésben annyi mondható el, hogy a biztonsági meghatalmazások és a SID-ek képezik az alapját a Windows biztonságának. A SID-ek az alap építőkövek, ezek segítségével ellenőrizzük, hogy engedélyezünk vagy tiltunk egy hozzáférést.

Autentikációs tár

Bármikor, amikor hitelesítenek bennünket, valamilyen formában tárolni kell, hogy futási időben össze lehessen vetni, hogy a hitelesítő mibe lép be, amikor meghatalmazást ad. A tárolási módok eltérnek attól függően, hogy milyen típusba tartoznak az autentikálók és hogy a tervezők hogy építették meg a rendszert. Számos tárolási módja van az autentikálásnak, a Windowsban leginkább a jelszavas védelem az elterjedt, gyakrabban használatos, mint a memóriakártyák, okos kártyák.

A memóriával rendelkező kártyák a tanúsítványon alapszanak. Ők maguk tartalmazzák a titkos részét a tanúsítványnak. A hitelesítő rendszer, ez esetben egy Active Directory tartománya tartalmazza a publikus részt. Ezért, amikor egy kártyát használunk, semmiféle kártyával kapcsolatos titkot nem kell tárolni a DC-kben. Ez a kártyák használatát a jelszóéval szemben egyszerűbbé teszi bizonyos helyzetekben.

A jelszóknak, gyakorlatilag minden implementációja ami elérhető, az megosztott titok. A titok, amit a felhasználó a bejelentkezéshez használ, az egyetlen és ugyanaz, mint amikor a szerver a felhasználó beléptetést autentikálja. Ezért a jelszavak elég érzékeny titok, és védeni kell őket. A korai időkben a megosztott számítógépes rendszerekben a jelszavak tisztán szöveggént voltak tárolva egy szöveges állományban. Azokban a rendszerekben még nem igazán volt cél, hogy távol tartsa a kívülállókat a jelszavaktól, mivel csak az emberek egy kis csoportjának volt belépési joga a rendszerbe.

Titkosítás és a Hash-elés

A titkosítás angol elnevezése (Encryption) a kriptográfia szóból ered, ami betűről betűre ugyanaz, mintha azt mondanánk, hogy rejtett írás. A titkosítás egy folyamat, mely során kriptográfiai módszereket felhasználva rejtünk el szöveget vagy alakítunk olvasható formából (sima szövegből) egy rejtett, titkosított formára. A titkosítás feloldása (Decryption) ellentétes irányú folyamat.

Amíg a titkosítás a kriptográfia használatával valamit egy olvashatatlan, de visszaírható formába konvertál, addig egy szoros kapcsolatban lévő folyamat, a hash-elés célja az, hogy a sima szöveget egy olvashatatlan és visszafordíthatatlan formába konvertálja. A hash-t például annak ellenőrzésére lehet használni, hogy összehasonlítsa két sima szöveget. Hogyha mindkettő ugyanazt a hash-t generálja, az egy elég nyomós indok, hogy azt feltételezzük, a két szöveg megegyező. A hash-re jellemző továbbá, hogy jóval kisebb (a sima szöveg arányában nő), mint egy titkosított szöveg.

Öt alapvető módja annak, ahogyan a Windows a jelszavakat tárolja, hogy autentikálni tudja a felhasználókat a Windowsba való bejelentkezéshez:

LM Hash

Az LM hash nem is egy hash tulajdonképpen, habár jó pár hasonló tulajdonsággal bír. Ez egy egyirányú folyamat, általában belső azonosításra használják, akárcsak a LMOWF funkciót (LanManager One-Way Function). Se a Windows Vistában, se pedig a Windows Server 2008-ban nem tárolják alapértelmezésként és nem is használják a hálózaton keresztül történő autentikációra. Habár meg kell jegyezni, a korai Windows verziókban mind tárolták és átörökölték. Talán emiatt érdemes lehet tisztában lenni az LM hash működésével. Vegyük észre, hogy mind a Windows Vistában, mind pedig a Windows Server 2008-ban be lehet állítani, hogy az autentikációt LM hash-sel tárolja, de az algoritmus gyenge pontjai miatt nem ajánlott a használata.

NT Hash

Amikor 1993-ban kijött az első Windows NT, egy új jelszótárolási módszer lett bejelentve. Jóval egyszerű mechanizmussal, mint az LM hash.

Jelszó Ellenőrzés

Ha már dolgoztunk a Windows Active Directory környezetben, valószínűleg észrevehettük, hogy magunkkal hozhatunk egy tartomány alapon csatlakozott laptopot, és autentikálthatjuk magunkat egy tartománybeli fiókkal, annak ellenére, hogy nem tartozunk a tartományba. Ez a kis varázslat egy olyan valaminek köszönhető, amit jelszó ellenőrzésnek hívnak. Ez a fajta ellenőrzés egy helyi másolata a tartományi jelszó hash-sének, amit arra használunk, hogy lokálisan csatlakozzunk. Az elmúlt években a támadók leginkább a jelszó ellenőrzésekre összpontosítottak. Ennek leküzdésére a Windows Vistában és Windows Server 2008-ban a jelszó ellenőrzés számítása meg lett változtatva.

A Memória

Amikor egy felhasználó bejelentkezik vagy valamilyen terminál szolgáltatást vesz igénybe, a Windows tárolja a jelszó hash-sét (az NT hash-et, és ha arra van beállítva, hogy tárolja, akkor az LM hash-et is). A hash-et a memória egy pontján tartja, ami csak az operációs rendszer számára elérhető, és természetesen bármelyik folyamatnak, ami úgy működik, mint egy operációs rendszer. Amikor egy felhasználó a hálózat egy olyan erőforrásához próbál hozzáférni, ami autentikációt igényel, az operációs rendszer ezt, a memóriában eltárolt hash-et fogja használni az autentikálásra. Ez az ami lehetővé teszi az egyenes autentikációt a hálózati erőforrásokhoz. Mihelyt a felhasználó kijelentkezik vagy zárolja a munkaállomást, a memória említett része automatikusan tisztul.

Visszafordítható Titkosítás

Végül, a Windowsnak van egy beállítási lehetősége, hogy a jelszót visszafordíthatóan titkosított szöveggént tárolja. Amikor ilyen módon tároljuk a jelszavunkat, vissza lehet írni sima szöveggé. Nyilvánvalóan ez azt jelenti, hogy semmilyen betörés nem szükséges. A visszafordítható jelszavak tárolása alaphelyzetben ki van kapcsolva, és általában csak két esetben használatos. Egyik, hogy ez szükséges, ha bizonyos régebbi autentikációs protokollt használunk távoli belépésre, ilyen például a CHAP vagy a Digest protokollok. Második, hogy ez szükséges, ha további bonyolultabb vizsgálatokat szeretnénk a jelszavakkal végezni, miután azok beállításra kerültek. Például valamilyen szervezet azt szeretné leellenőrizni, hogy a jelszavak tartalmazznak-e bizonyos szavakat. A szervezetnek visszaírható formában kell tárolnia a jelszavakat.

Autentikációs Protokollok

Talán a jelszavak tárolásánál kicsit fontosabb az, ahogyan azokat utána felhasználják. A jelszavak a feljogosítók – őket használjuk arra, hogy autentikálják a felhasználót a számítógéphez. Hogyha a felhasználó bejelentkezik egy helyi fiókra, a folyamat elég egyszerű:

1. A felhasználó a Secure Attention Sequence-t (SAS, úgy is ismert, hogy három ujjas tisztelegés, Ctrl+Alt+Delete) használja, hogy feljöjjön a bejelentkező párbeszédablak. Ez elindítja a Local Security Authority Sub-System rendszert (LSASS), az létrehoz egy új munkamenetet és betölti a WinLogon-t ebbe a munkamenetbe. A WinLogon sorjában betölti a LogonUI-t.
2. A felhasználó beírja nevét és jelszavát.
3. A WinLogon folyamat felhasználja a jelszót, hash-seli egy NT hash-be, megkeresi a felhasználónevet a helyi SAM-ben, és összehasonlítja az NT hash-t azzal, ami tárolva van a felhasználónak. Ha azok egyeznek, a bejelentkezés sikeres.
4. Ha al-authentikációs csomagok telepítve vannak a számítógépre, akkor a bejelentkezési információk további feldolgozásra továbbítódnak hozzájuk. Különben a user32.exe meghívásra kerül, és betöltődik a felhasználó környezete.

Ez a folyamat elég egyenes, mert egész végig létezik egy biztonsági csatorna a LogonUI-től kezdve, ami beveszi a sima szöveget, amit a felhasználó begépel, az ellenőrzésig. Azonban ha az autentikációt a hálózaton keresztül megy végbe, akkor ez a folyamat kicsit bonyolódik, mert azzal is törődni kell, hogy az autentikációs igények átvitele megfelelő legyen a kliens géptől, ahol a felhasználó ül, a szerverig, ami a fiókok adatbázisát tárolja.

A jelszavak és az autentikáció egy nagyon érdekes terület. Nem kell egy autentikáláshoz értő embernek lennünk, hogy Windows szervereket kezeljünk, de elég hozzáértés kell az alapfogalmakhoz, hogy intelligens döntéseket hozzunk autentikálással kapcsolatban. A kezeléssel kapcsolatos rossz döntéseknek köszönhetően nem egy hálózatot tettek tönkre vagy törtek fel. Csak azzal tudunk megindokolt döntéseket hozni a birodalmunk védelme érdekében, ha van elég elképzelésünk az autentikáció működéséről.

Személyes értékek

Megvédhető tárgyak

Bármilyen dolog, amire vonatkozóan létezhetnek jogosultságok. A legvalószínűbb eset, amivel dolgozhattunk eddig, az a fájl volt. Az NTFS rendszerekben a fájlok és a könyvtárak mind rendelkezhetnek hozzájuk társított jogosultságokkal. Gyakorlati kérdésként, a jogok tulajdonképpen a fájlrendszer meta-adatában tárolódnak, nem magában a fájlban – de ez egy olyan technikai kérdés, ami nem számít egy rendszer adminisztrátornak.

Különböző dolgok, melyeket meg szeretnénk védeni, a következők lehetnek:

- Fájlok
- Könyvtárak
- Registry kulcsok
- Active Directory objektumok
- Kernel objektumok
- Szolgáltatások
- Szálak
- Folyamatok
- Tűzfal portok (újonnan a Windows Vistában és Windows Server 2008-ban)
- Windows állomások és asztalok

Security Descriptor-ok

Minden megvédendő tárgynak van egy közös tulajdonsága: van hozzájuk társítva egy biztonsági leíró (SD). Az SD egy olyan dolog, ami minden a tárgyhoz kapcsolt biztonsági információt tartalmazza. Ábrázolása egy 5 soros táblázat, soronként 32 bit információval. Melyből 4 sor mutatókat tartalmaz, a tulajdonosra, a csoportra, SACL-re mutató (System Access Control List) és DACL-re mutató (Discretionary Access Control List).

Felhasználó Fiók Felügyelet (UAC)

A számítógép nyújtotta lehetőségek színvonalának emelkedésével, mint például banki tranzakciók végrehajtása, online vásárlások lebonyolítása, személyes információk tárolása és megosztása, egy sor új fenyegetés született a biztonságra. A Windows userek nagy számban adminisztratív jogokkal használták a számítógépüket. Hogyha ezek a felhasználók véletlenül valamilyen rosszindulatú szoftvert (malware-t) telepítettek a gépükre – aminek így adminisztrátori hozzáférése volt – gyakorlatilag bármit tehetett. A Windows Vistában és Windows Server 2008-ban újonnan megjelent User Account Control (UAC) arra lett tervezve, hogy a „legkisebb jogúság” elvét tekintse alapnak. Csak éppen elegendő hozzáférést biztosít ahhoz hogy elvégezzük a feladatot. Ez a beépített adminisztrátort kivéve minden felhasználót érint. Ez egyszerűen hangzik, de széleskörű változtatásokat foglal magában, egészen az operációs rendszer magjában.

Mi az az UAC?

Az UAC abban segíthet, hogy megakadályozzunk illetéktelen változtatásokat a számítógépen, azzal, hogy a cselekménye történése előtt a felhasználó jóváhagyását kéri. Amikor egy magasabb jogokkal felruházott felhasználó lép be a Windows Vistába vagy Windows Server 2008-ba, két hozzáférési token kerül kiosztásra: egy teljes hozzáférésű token és egy korlátozott szabványos felhasználói hozzáférés token. Egy szűrő folyamat elveszi az adminisztratív jogokat, és kikapcsolja az Adminisztratív csoport Biztonsági Azonosítókat (SID-eket), eredményül adva a korlátozott szabványos felhasználói hozzáférés tokent. A szabványos felhasználói tokent azután arra használja, hogy elindítsa a Windows asztalt (explorer.exe) és a további gyermek folyamatokat. Következésképpen minden alkalmazás a szabványos felhasználói tokennel indul alaphelyzetben, és csak akkor fog teljes hozzáférésű tokent kapni, amikor egy adminisztrátor jogokkal ruházza fel. Figyeljünk arra, hogy mivel egy alkalmazás örökli a szülője jogainak szintjét, azért ha a szülő teljes körű jogokkal fut, az új gyermeke azt fogja örökölni anélkül, hogy kérné az engedélyeket az adminisztrátortól. Például, ha adminisztrátorként parancssorból indítunk alkalmazásokat, mindegyik adminisztrátori joggal fog elindulni.

Mi új a Windows Vista SP1 és Windows Server 2008 UAC-jában

Új csoportháztípus beállítás: UIAccess alkalmazások előléptetése Secure Desktop használata nélkül.

Ez a beállítás lehetővé teszi az UIAccess alkalmazásoknak (például Remote Assistance), hogy a secure desktop indításait kikapcsolja. Amikor az UIAccess alkalmazás befejeződött, azok automatikusan újra engedélyezésre kerülnek. Ez egy kényelmes megoldás mindazon vállalatoknak, amik a Remote Assistance-re számítanak, hogy gondoskodjanak a végfelhasználók asztali segítségnyújtás támogatásáról. Ez a beállítás alaphelyzetben ki van kapcsolva.

UAC felszólítások csökkentése ha fájlműveletet hajtunk végre Windows Explorerrel.

Ha a felhasználó egy védett területen hoz létre új mappát, a felhasználót csak egyszer kérdezzük meg a létrehozásról és elnevezésről. Ez egy kétszeres kérdés volt a Windows Vista RTM-ben.

Több, mint 40 UAC-hoz kapcsolódó kompatibilitást növelő alkalmazás

Az UAC team az alkalmazást fejlesztő team-mel közösen 40-nél is több új alkalmazást gyártott, ami segít a Windows Vista és Windows 2008 kompatibilitásának növelésében.

UAC a gyakorlatban

Az UAC kezelése nem olyan nehéz, mint amilyennek tűnhet. Egy szervezetnél való kibontakozásunk javarészt attól függ, hogy a szervezet milyen biztonsággal kapcsolatos követelményeket támaszt, és hogyan valósítja meg a szükséges politikát azok kielégítésére. A biztonsági értéktől függően jó, jobb, legjobb megoldásokat lehet felsorolni.

Gyakorlatban jó

A felhasználót Admin jóváhagyással futtatja. Ha egy adminisztratív felhasználónak magasabb jogokra van szüksége, a vállalat UAC politikája arra kényszeríti, hogy érvényes adminisztrátor felhasználónevet és jelszót ír be, ahelyett, hogy a hozzájárulós párbeszéd ablakon kattintana. Ez a beállítás megakadályozza az illetéktelen felmagasztalást azon csekély számú esetben, amikor a felhasználó gazdátlanul hagyja a munkaállomását. A biztonság növelése érdekében megkövetelhetjük a Ctrl+Alt+Delete billentyűkombinációt bármilyen

fentebb minősítés elvégzéséhez. Ez az adminisztratív jogok igazolásának beírását még biztonságosabbá teszi.

Gyakorlatban mégjobb

Követeljük meg, hogy a felhasználóknak, akiknek adminisztrátori jogokra van szüksége, legyen két fiókjuk: egy szabványos fiók a mindennapi cselekvésekre, akár csak az e-mail olvasás, és egy az alkalmi adminisztratív műveletekre. A szabványos felhasználó beléphet, és ha szükséges, jogokat emelhet az UAC meghatalmazás indíttatásával. Ez nem a legszerencsésebb eset, mert így a felhasználó mind szabványos, mind adminisztrátori előjogos módban futtatja az alkalmazásait a munkamenetében. A biztonság növelése érdekében a vállalat arra kényszerítheti a felhasználót, hogy kötelező legyen használni a gyors felhasználók közötti váltást (Fast User Switching, FUS) amikor csak egy magasabb jogokat igénylő műveletre kerül a sor. Annak ellenére, hogy FUS sokkal biztonságosabb, megvannak a maga hátrányai. A biztonság növelése érdekében szintén megkövetelhetjük a Ctrl+Alt+Delete billentyűkombináció használatát.

Gyakorlatban a legjobb

Minden felhasználót szabványos felhasználóként futtatni. Az informatikai osztálynak így azt kell elfogadni, hogy a szabványos felhasználóknak általánosságban nem lesznek jogaik ahhoz, hogy alkalmazásokat telepítsenek. A Windows nyújt egy telepítéssel kapcsolatos szolgáltatást, ami neve a Microsoft Software Installer (MSI) Service. Továbbá a Group Policy Software Installation (GPSI) bővítmény lehetővé teszi, hogy alkalmazásokat osszunk ki a felhasználóknak azok interakciójának szükségessége nélkül.

Az UAC valószínűleg a legtöbbet tárgyalt jellegzetessége a Windows Vistának. Még a rivális értékesítő ügyfelek hirdetéseinek is témája. Nehéz eldönteni hogy áltassuk vagy idegeskedjünk, a Microsoft konkurensei már még kíváncsabbban hirdetik a terméküket, mert a Windows túl biztonságos. A régi állapot, amikor a felhasználók adminisztrátorként tevékenykedtek, elfogadhatatlan és országos malware járványhoz vezetett. A jövő egy irányba vezet, a felhasználók csak akkor használnak adminisztratív jogokat, ha szükséges. Az UAC egy lépés ebbe az irányba, de csak akkor működik, ha az emberek használják. Kivehetjük a részünket az informatikai ökoszisztéma védelmében, ha olyan szoftvert vásárlunk, amely támogatja ezt a funkciót, és olyat visszautasítunk, amely nem.

Tűzfal

Aki akkor született, amikor még a zenét analóg formában vinilre rögzítették, az emlékszik hogy a számítógépeket folyamatos internet kapcsolat nélkül, de egyáltalán még csak hálózathoz se kapcsolva használta. Ahogyan manapság a hálózati technológia a laborból a szobánkba költözik, úgy kezdik az emberek felfogni az illetéktelen hozzáférés és sima szöveg alapú kommunikációs protokollok következményeit. Olyan, mintha egy elképesztő kihívást jelentő macska-egér játékot játszanánk gonosz céllal. Sajnos a jófiúk túl gyakran az egerek.

Az első tűzfalak a késő '80-as években jelentek meg válaszként a biztonsági betörésekre, mint például a Morris féreg. A korai tűzfalak a mostani fejlesztésekhez képest egyszerűek voltak: Átengedték vagy blokkolták a bejövő forgalmat attól függően, hogy milyen információ volt a csomag fejlésében, gondolni kell itt a forrás IP-re vagy a port számra. Nem követték nyomon a kommunikáció sorrendjének állapotait a központi hálózat megbízható kiszolgálója és a másik oldali anonim között. Az első tűzfalak alaposak voltak – megértették a csomagok normál sorrendjét, amiket arra használtak fel, hogy felépítsék és megtartsák a kommunikációt két befogadó host között. Ezután felbukkantak a hozzáértő alkalmazási réteg protokollok: Tulajdonképpen megfigyelték a csomag tartalmát, ártalmas forgalom után kutatva. Például egy Webszerver védő tűzfal megvizsgálhatott egy HTTP kérést egy távoli klienstől kapva, hogy eldöntse, az egy legitim kérés valamilyen adatért vagy egy kísérlet, hogy veszélyeztesse a szervert. Az alkalmazási rétegbeli tűzfalak emiatt nagyon kifinomultak lettek; bárki aki érti, hogy a Microsoft Internet Security vagy az Acceleration Server (ISA Server) mit csinál amikor egy olyan szervert védelmez, ami a Microsoft Office Outlook webes hozzáférését látja el, az felismeri mennyire erőteljesek a technika lehetőségei.

A rengeteg mobilkészülék és egyre komplexebb hálózati architektúrák miatt, ahol nélkülözhetetlen üzleti információk áramlanak a nyilvános interneten keresztül, a legtöbb szervezet a host alapú tűzfalakat is telepíti. Az autentikáció és a titkosítási technológiák is jelentős mértékben fejlődtek. A távoli kiszolgálók is biztonságos kapcsolatokat építenek ki már, köszönhetően a Transport Layer Security (TLS)-nek, Internet Key Exchange (IKE)-nek és egyéb protokolloknak. Számos módon képesek autentikálni a felhasználókat; és titkosítani is képesek a hálózat forgalmát, a Protocol Security (IPsec), Secure Hypertext Transport Protocol (HTTPS) és egyéb protokollok használatával. A Windows Server 2008 a legtöbb ilyen protokollhoz támogatást nyújt.

A megnövelt biztonságú Windows tűzfal

A kapcsolat kiépítésének lehetősége mindenütt jelen van. A legtöbb számítógép nem csak egy helyi hálózathoz kapcsolódik, de az Internethez is. Mindenütt nagysebességű vezeték nélküli hálózatok és mobil felhasználók vannak, kitéve a malware-ek és mérhetetlenül kibocsátott spam áradatok gazdájául szolgáló internet nyújtotta veszélynek. Még a jól kezelt hálózatok szerverei is veszélynek vannak kitéve a visszatérő utazók miatt, akik a laptopjaikkal csatlakoznak, amik az útjaik alatt megfertőződtek; a konzulensek és vásárlók miatt, akik a hálózat megosztását kérték, és természetesen rosszindulatú belső emberek miatt is, akiknek akármilyen indokkal is, de a legfőbb érdekük, hogy kihasználják az üzleti rendszerünket.

Ezen okokból kifolyólag érdemes fontolóra venni a host alapú tűzfalak használatát a Windows Server 2008-ban, hogy még egy védelmi réteggel szolgáljunk a mély védelmi vonalunkon. A megnövelt biztonságú Windows tűzfal egy kétirányú szűrővel van ellátva, ami segít a nem kívánatos forgalom bejutásától megvédeni rendszer futó folyamatait, és megakadályozni a veszélyt jelentő szerverek támadásait a hálózatunk további részein. A Windows tűzfal és a Internet Protocol Security (IPsec) kezelése bele lett építve az MMC konzolba (Microsoft Management Console), hogy a tűzfalak a hálózat-védelmi stratégiánk alapkövei lehessenek.

A Windows tűzfal javításai

Jobb kezelőfelület

A legjelentősebb újítás az új grafikus kezelőfelület, hogy a Windows tűzfal helyi- és Active Directory-n keresztüli tartományalapú csoport politikájának kezelése könnyebb legyen. A régi vezérlőpultbeli elem, a Windows Tűzfal még mindig nyújt belépést az alap vezérlőkhöz. Az új felhasználói kezelőfelület a Microsoft Management Console (MMC) konzolba épül be. A helyi beállítások kezeléséhez jogunk van a megnövelt biztonságú Windows tűzfal konzoljában, az adminisztratív eszközök mappában. Ez a beépülés része továbbá a csoportházirend szerkesztő konzoljának, az Active Directory tartománybeli csoportházirend szerkesztése miatt. Fejlesztések történtek továbbá a netsh.exe-ben, a command-line-ban a tűzfal és IPsec kezelése miatt. A netsh parancs is bővült, az advfirewall arra való, hogy a tűzfal beállításait írassuk be vagy hogy a szerver magjába telepítést bonyolítsuk le.

A Windows Service Hardening

Bár rengeteg lépés történt, hogy megvédjük magukat a szolgáltatásokat, egy támadó valószínűleg még mindig talál valamilyen módot, hogy kihasználjon egy Windows rendszerbeli szolgáltatást. Ha egy szolgáltatás veszélyeztetett, a Windows Service Hardening segít, hogy számos módon csökkenteni lehessen a kihatását: A tűzfal blokkolja a rendellenes viselkedést, például egy szolgáltatást, ha nem kellene a hálózatra csatlakoznia és HTTP forgalmat lebonyolítania.

Kifele irányuló forgalom szűrése

A Microsoft új szerverének operációs rendszere intelligensen használja a kifele irányuló forgalom szűrését azzal a technikával, hogy szolgáltatásokat blokkol a hálózati kapcsolatok kezdeményezésében, kivéve azokat amelyekre szüksége van a helyes működéséhez. Ha egy szolgáltatást mások kihasználnak valamilyen céllal, nem lesz joga a tűzfal átkonfigurálásához anélkül, hogy figyelmeztetné a felhasználót, mert meg van neki tiltva a tűzfal beállítások módosítása. Alaphelyzetben az új tűzfal minden egyéb kimenő csomagot engedélyez. Meg lehet változtatni az alap viselkedést, hogy blokkoljon minden kimenő forgalmat, de nem ajánlatos, mert órákat, napokat, de talán heteket tölthetünk el azzal, hogy kitaláljuk a kivételeket, amiket engedélyezni kell, hogy a szerver úgy működjön, ahogyan kell neki.

Egyéb szabályok

A Windows Server 2008-ban és Windows Vistában a tűzfal mind a kifele és mind a befele irányuló forgalomra be van kapcsolva. Az alapelv szerint blokkolva van a legtöbb bejövő forgalom és engedélyezve a legtöbb kimenő. A tűzfal támogatja bármilyen IP protokoll szám szűrését, ellentétben a régebbi Windows XP tűzfallal, ami csak a Transmission Control Protocol (TCP), User Datagram Protocol (UDP), és az Internet Control Message Protocol (ICMP) forgalom szűrését támogatta. Lehetőségünk van egyedi beállításokra, amikkel a forgalmat blokkoljuk vagy engedélyezzük IP címek használatával, IP protokoll számokkal, Active Directory szolgáltatás felhasználók és csoportokkal, rendszer szolgáltatásokkal, UDP és TCP forrás és cél porttal, specifikus interfészekkel, és ICMP-vel típus és kód szerint.

A helyének tudatában levő profilok

A Windows tűzfal előnyt kovácsol a TCP/IP új tulajdonságából, ami az útvonalat, hogy a hálózat mihez csatlakozik veremszerűen tárolja. Szabályokat és beállításokat konfigurálhatunk mindhárom profilfajta: Tartomány, Privát, Publikus. A tartományi profil lép életbe, ha minden a hálózatba tartozó gép hálózatának van Active Directory tartományvezérlője. A privát profilt akkor használják, ha minden aktív hálózat a rendszergazda által ki lett választva, mint privát, amit tűzfal véd. Publikus profilról akkor beszélünk, ha a számítógép közvetlenül kapcsolódik az internethez, vagy a hálózat nem privát vagy tartománybelinek lett definiálva.

Felhatalmazás a szabály kikerülésére

Beállíthatunk olyan szabályokat, hogy egyedi számítógépek valamely csoport számítógépei közül kikerüljék más tűzfalak szabályait az IPsec autentikációt felhasználva. Ez azt jelenti, hogy blokkolhatunk egy bizonyos fajta forgalmat minden más kiszolgálótól, de engedélyezhetjük pár rendszer kiválasztását, amik ezt a korlátozást figyelmen kívül hagyják és hozzáférnek a blokkolt szolgáltatáshoz. A szabályok még specifikusabbak lehetnek, ha azt is hozzávesszük, hogy milyen portok vagy programok fogadhatják a forgalmat.

A Windows tűzfalának kezelése

A vezérlőpultból elérhető Windows tűzfal applet csak pár alapvető beállítás módosításában tud segíteni, a javított funkciók módosításához a megnövelt biztonságú Windows tűzfal MMC konzolját kell használni, vagy a csoportházirend szerkesztő MMC konzolját, de a netsh paranccsal parancssorból is elvégezhetők a beállítások. A megnövelt biztonságú tűzfal konzoljával nem csak a helyi kiszolgáló, de távoli számítógépeket is konfigurálhatunk.

IPsec (Internet Protocol Security)

AZ IPsec alapjai

Az IPsec (Internet Protocol biztonság) egy nyílt alap, melyet az adatszállító hálózatok védelmére használnak az illetéktelen behatolás és módosítás ellen. Ezt az autentikációs protokollok, adat titkosítás és digitális aláírások kombinációjával éri el. Amikor két host IPsec alapú kommunikációt indít, a kezdetkor kiépítenek egy biztonsági kapcsolatot. Az egyes fázisban vagy fő eljárásban, a host autentikál egy másikkal, a kettes fázisban vagy gyors eljárásban a hostok egyeztetik, hogy milyen protokollokat fognak a hálózati fogalom digitális aláírására illetve titkosítására használni. Minden csomagon jelezhetünk, hogy a fogadó host biztos legyen benne, semmilyen módon nem lett módosítva és megbízható forrásból érkezik. Bármelyik csomagot titkosíthatjuk, hogy megvédjük az adatot a cél kiszolgálótól eltérően bárki hozzáférésétől. Az IPsec szabályait beállíthatjuk, hogy ezen védelmi formák valamelyikét vagy mindegyikét megvalósítsa.

Az IPsec autentikációja

A biztonsági kapcsolatok egyezményesen az IKE (Internet Key Exchange) protokollt használják, ami magában három másik protokollt tartalmaz: ISAKMP, Oakley és SKEME. Az IKE-en keresztül a két host megállapodik, hogy az autentikációs üzenet hogy fog felépülni és cserélődni. A hostok az autentikációt több fajta módon is elvégezhetik, beleértve a következőket:

- *Kerberos version 5* – Ha a két host azonos Active Directory erdőben található, a Kerberos-t használhatja a kölcsönös autentikációhoz. Használata ideális, ha nincs PKI-nk (public key infrastructure) és a megbízott hostoknak nincs ezen erdőn kívülre kiépített kapcsolata.
- *Digitális igazolás* – Ha a hostoknak egy robosztus PKI-hez kell csatlakozni, ez a megfelelő autentikálási módszer. A Windows XP és későbbi verziói a Microsoft operációs rendszereknek automatikusan támogatja az igazolások elosztását, ami a legtöbb erőt igénylő kihívása a nagy PKI kezelésének: elosztott igazolások. Amíg mindegyik hostnak van egy igazolása egy más által megbízhatónak vélt Certificate Authority (CA) által aláírva, addig az másnak is autentikálhat.

- *Előre megosztott kulcsok* – Ezen módszer támogatása csak az IPsec szabványnak való megfelelés miatt került be. Az egyetlen helyzet, amiben ennek a módszernek van értelme, amikor fejlesztjük és teszteljük az IPsec házirendünket. Minden host, aki ebbe a házirendbe beletartozik, kötelezően rendelkezik egy ugyanolyan kulccsal. Mint ahogy több felhasználó ugyanazzal a jelszóval is egy rossz ötlet, több gép közötti azonos kulcs megosztása autentikáció céljából is.

Az IPsec kommunikációk fajtái

Az IPsec kommunikáció két módban történhet: vagy Transport vagy Tunnel mód.

A Transport mód megfelelő, ha azt szeretnénk, hogy több számítógép IPsec-et használjon egymással. Ebben a módban a két host egy másikkal autentikál az első fázisban, aztán megegyeznek a forgalom aláírás és titkosítási eljárásokról.

A Tunnel mód alkalmas a hely a helyhez csatlakozó kapcsolatok védelmekor, amik egy nem megbízható hálózaton mennek keresztül, mint például az internet. Más szavakkal a két host egy-egy kapu, ami forgalmat irányít a helyek között. A kapuban a kimenő forgalom titkosításra kerül, és a másik kapuhoz lesz elküldve, ahol dekódolják és elirányítják a belső hálózatban a végleges helyéhez.

A Windows Server 2008 új képességei

A Windows Server 2008 számos újítást hozott az IPsec terén, ezek a következők:

- Integrált tűzfal és IPsec beállítás
- Egyszerűsített IPsec házirend és beállítás
- Javított IPsec autentikáció
- Javított terhelés kiegyensúlyozás és csoportosított szerver támogatás
- Kliens-DC IPsec védelem
- Beépített IPv4 és IPv6 támogatás
- A Network Access Protection (NAP) integrációja
- További beállítási lehetőséggel a védett kommunikációhoz

- Új kriptográfiai támogatás
- Hálózati diagnosztika keretrendszer támogatás

Network Access Protection

A Network Access Protection (NAP) egy platform, kikényszeríti a rendszer egészségének előfeltételét a hostokon ahhoz, hogy engedélyezve legyen a hálózati erőforrásokhoz a hozzáférése. A NAP biztosíthatja, hogy a rendszer eleget tegyen egy bizonyos korszerűségi szintnek és beállítási követelményeknek, mint például a tűzfal állapota. A NAP azt is biztosíthatja továbbá, hogy konkrét szoftver, például antimalware telepítve legyen és naprakész legyen. A Windows Server 2008-ba be vannak építve a szerver komponensek, amelyek szükségesek a NAP-hoz. Szintúgy NAP kliens lehet, mint ahogy a Windows Vista, Windows XP és Windows Server 2003 – habár az utóbbi kettő 2008-as Microsoft frissítéseket igényel. Az egészségi házirend definiálja, mely frissítések, antimalware aláírások, szoftver verziók, biztonsági- és egyéb beállítások szükségesek a NAP kliensen, hogy az elérhesse a hálózati erőforrásokat. A feltételeknek eleget nem tevő rendszereknek csak limitált hálózati hozzáférése van, ahol olyan változtatásokat tehetnek, amilyeneket csak szükségesnek tartanak, hogy eleget tegyenek a feltételeknek.

A NAP működése

A NAP úgy lett tervezve, hogy az adminisztrátor beállíthassa, milyen követelményeknek kell megfelelni, ezért az aktuális beállítás az adminisztrátortól függ, habár a NAP alapja ugyanaz marad. A működési elv a következő:

- Egészségi állapot validáció. Egészségi követelmények teljesítése
- Beállítások (példa: IPsec, 802.1X, VPN, DHCP)

A feltételek teljesítése alapján, a felsorolt beállítások egyeznek (autentikált 802.1X, VPN kapcsolat az intranettel, ...) besoroljuk a NAP klienst:

- Feltételeknek eleget tevő, korlátlan kapcsolat
- Feltételeknek eleget nem tevő, limitált kapcsolattal. Nem feltétlenül jelenti azt, hogy vírust tartalmaz vagy egyéb fenyegetést a kliens, de azt jelenti, hogy nem feleltek meg

a beállítások a feltételeknek, emiatt egy magasabb kockázattal állna szemben az intranet. A korlátozott hálózat fizikailag vagy logikailag értendő – például IP szűrő, statikus routolás, ACL vagy VLAN.

A legtöbb intranet komponensek és készülékek heterogén keveréke. Az adminisztrátor felmenthet számítógépeket az egészségi feltételek alól, olyanokat, amiknek korlátlan kapcsolatra van szüksége, régebbi Windows verziókat, melyek nem is támogatják a NAP-ot. A nem NAP kompatibilis számítógépekre külön szabályt alkothat a rendszergazda a teljes elérés érdekében. Célszerű azonban frissíteni ezeket a rendszereket NAP kompatibilissé.

A NAP szükségessége

A számítógép folyamatosan ki van téve a tejredő káros szoftverek, malware-ek fenyegetettségének. A NAP központilag meghatározott egészségi követeléseket támaszt, hogy a privát hálózatot megvédje a támadásoktól.

A malware és kihatása egy vállalati számítógépen

Szomorú tény az életben, hogy a modern számítógépek ellenséges környezetek. A hasonló számítógépes hálózati technológiák, amik csomópontok nélküli kommunikációt tesznek lehetővé levelezésre, fájl küldésre, Webes elérésre, azok is ki vannak használva a malware-ek által, hogy belépjenek és megfertőzzenek sebezhető gépeket. A malware úgy van tervezve, hogy a felhasználó tudta és beleegyezése nélkül települjön a számítógépre, abból a célból, hogy kárt okozzon, adatokhoz hozzáférjen, a számítógép tevékenységeiről jelentést küldjön és így engedélyezzen egy másik számítógépet, hogy átvegye az irányítást. A malware formailag megjelenhet Vírusként (programok, amik más gépekről származnak, a hálózaton vagy média cseréléseken keresztül terjed) Trójaiak (malware-ek belerejtve más programokba, amiknek amúgy más céljai vannak) Spyware-ek (malware, ami feljegyzi és jelenti, ahogyan a számítógépet használják) vagy Adware-ek (malware, ami hirdetéseket jelenít meg a felhasználónak).

Az internet egy különösen veszélyes övezet, ahol egy gyenge számítógépet percek alatt támadhatnak és fertőzhetnek meg cím- és portvizsgáló malware-ek. Az otthoni hálózatok szintén veszélyes környezetet alkotnak, nem csak a címet és portot vizsgáló malware-ek

veszélyeinek vannak kitéve, de hálózattól jövő valamely gépre már eleve installált malware-eknek is, trójai technikával, e-mailen vagy ingyenes szoftvereken keresztül feljutva.

A privát, szervezeti hálózatok, ismertebb nevükön az intranetek, kevesebb veszélynek vannak kitéve, mivel jellemzően nem csatlakoznak az internethez. Továbbá, legalábbis a vállalati hálózatban, egy IT csapat rendelkezik malware ellen fejlesztett szoftverrel. Ennek ellenére a vállalati hálózatok még mindig ki vannak téve a trójai alapú szoftverek támadásainak, amiket a felhasználók töltenek le az interneten keresztül.

Ahogy a malware bejut a vállalati hálózatba

Jellemzően az ilyen hálózatok nincsenek közvetlen kapcsolatban az internettel. Létezik egy kisebb számítógép csoport, amelyek közvetlenül kapcsolódik, hogy szolgáltatssa az internet kapcsolatot a felhasználóknak vagy üzletfeleknek. A legtöbb intranetbeli számítógép szeparálva van az internettől elkerítő rendszerekkel, például tűzfalakkal, proxy szerverekkel. Ennek ellenére a következők ki tudják játszani a proxy szerverek és tűzfalak által biztosított elkerítést:

- *Trójai alapú vírusok, melyek kód formában kerülnek fel, azután végrehajtásra a számítógépen* – A vállalati hálózat felhasználói nem szándékosan kaphatnak vírust e-mailből, web oldalakról, bármilyen fájlból, amit az internetről töltek le. Az e-mailben történő fájlcsatolás közkeletű módszere a trójai alapú vírusok terjesztésének.
- *Mobil számítógépek, melyeket lehet mozgatni és más hálózatokhoz csatlakoztatni* – Nyilvánvaló példa a mobil számítógépre egy laptop. A felhasználó hazaviszi a laptopját, üzleti utakra hurcolja, valamint egyéb nyilvános helyekre, ahol van vezeték nélküli hálózat. Mindenegyed alkalommal, amikor nem a vállalati hálózatra csatlakozik, felvállalja a kockázatot, hogy hálózati szintű vírusoknak teszi ki a számítógépet.
- *Alkalmazottak távoli elérése* – Amikor az alkalmazottak távoli kapcsolatot használnak, hogy a vállalat hálózatába kapcsolódjanak, akkor logikailag kapcsolódni tudnak, mintha egy ethernet kábelt használva a vállalati hálózat egyik switch-jéhez

kapcsolódnának. Ezen a fajta kapcsolaton keresztül a szervezet hálózati szintű vírusoknak lehet kitéve.

- *Vendég számítógépek* – Amikor a szervezet vendégei – mint például tanácsadók, eladók vagy üzleti partnerek – számítógépeikkel csatlakoznak szintén vírustámadások veszélyeinek teszik ki a hálózatot.

Malware támadás

A malware-nek közvetlen anyagi kihatása is lehet a hálózati munkára, mind az internetes, mind a belső hálózatokra, a bizalmas információk kiszivárgása, szellemi tulajdon elvesztése, sávszélesség felhasználása és a malware által tönkretett gépek használhatatlansága miatt, továbbá az idő miatt is, amit az eltávolításukra fordítani kell. A malware hálózati kommunikációkat rombolt szét a múltban, és megvan a lehetőség, hogy a jövőben is fog.

A megnövelt biztonsággal rendelkező Windows tűzfal az új host alapú tűzfal, ami szorosan integrálódik az IPsec-cel és a NAP-pal. Használhatunk izolációs szabályokat a NAP-pal és IPsec-cel kapcsolatban, hogy megvédjük a szervereket a potenciálisan veszélyes hálózati host-októl. Javítások történtek az RRAS szolgáltatásban is. Ezeket a technológiákat mind használhatjuk, hogy elősegítsük a kommunikációt a hálózati host-ok között, miközben a gonosz kezek veszélyeztetéseit minimalizáljuk.

Szolgáltatások

Mi a szolgáltatás?

Annak a megértése, hogy egy szolgáltatás miben különbözik egy normál alkalmazástól fontos, hogy megértsük magukat a szolgáltatásokat. A legtöbb Microsoft által telepített Windows szolgáltatás DLL-ek és EXE-k formájában töltődnek be, a \System32 könyvtár alatt helyezkednek el, de bármelyik érvényes helyi meghajtó könyvtárban lehetnek. A szolgáltatások a 0. munkamenetben indulnak, a rendszerrel együtt, adatvégrehajtás megelőzés (Data Execution Prevention, DEP) ki van kapcsolva, SID-del együtt (SERVICE security identifier) valamint a fájl- és registry virtualizáció is ki van kapcsolva.

Service Log-on Account

Minden szolgáltatáshoz tartozik egy service log-on account, ami meghatározza az elsődleges biztonsági környezetet, amiben a szolgáltatás fut. A beépített service log-on account-ok a helyi rendszer, helyi szolgáltatás és hálózati szolgáltatás; de az adminisztrátoroknak és fejlesztőknek joga van csinálni és használni új, saját account-ot. A jogok, meghatalmazások és előjogok account-hoz csatolása egy elsődleges (de nem egyedüli) módszere annak, hogy meghatározzuk milyen helyi vagy hálózati erőforráshoz tartozó használati jogai vannak egy szolgáltatásnak. A szolgáltatások használhatják a beépített service log-on account-okat, vagy használhatnak érvényes helyi- vagy tartománybeli account-ot. A Windows-ok korai verzióiban minden Microsoft által létrehozott szolgáltatás a helyi rendszeren futott. Sajnos ez a politika nem követi a legkisebb jogúság elvét. A Windows XP-től kezdve a Microsoft a jobban korlátozott helyi szolgáltatások és hálózati szolgáltatások létrehozását támogatja, és lassan elkezdte lépésenként követni a legkisebb jogú modellt, a szolgáltatások fejlesztése és telepítésekor. A Windows Server 2008-ban a szolgáltatások 58%-a fut a helyi rendszeren, ezt követi a helyi szolgáltatás 26%-kal, végül 16%-kal a hálózati szolgáltatás.

A service log-on account-ok arra valók, hogy szolgáltatásokhoz autentikáljunk helyi vagy távoli erőforrásokat. Az SPN (Service Principal Names) arra való, hogy egyértelműen azonosítsa egy szolgáltatást, elfogadva egy kölcsönös autentikációt a kliens alkalmazás és a szolgáltatás között. A szolgáltatásoknak, amelyek Kerberos autentikációt szeretnének használni, rendelkezniük kell egy vagy több SPN-nel a service log-on account-hoz csatolva.

Támadások a szolgáltatások ellen

Mivel a Windowsnak sok-sok szolgáltatása van, melyek automatikusan indulnak a rendszer minden egyes bootolásakor, a rosszindulatú hackerek tudják, hogy ezek nagy valószínűséggel érhetőek el, emiatt gyakran célozzák ezeket.

A Blaster féreg

Talán a leghírhedtebb Windows szolgáltatás támadás az úgynevezett Blaster féreg volt. A Blaster a Windows DCOM RPC egyik ismert gyengeségét, a puffertúlsordulást támadta a

Windows 2000-ret vagy Windows XP-t használó számítógépeken. Habár a gyengeség ismert volt és egy Microsoft biztonsági frissítés is rendelkezésre állt, a Windows gépek nagy százaléka mégsem volt frissítve. A védelem hiányához egy félreértett elgondolás is hozzájárult, miszerint a "jól beállított" kerületi tűzfalak megakadályozzák a Blaster féreg betörését az közösségi hálózatba. A Blaster féreg úgy működött, hogy csatlakozott a DCOM RPC szolgáltatáshoz a TCP 135-ös portján és egy puffertúlcsorduláson alapul támadást idézett elő. Amikor a szolgáltatás túlcsordult, a Blaster féreg hozzáférést adott a helyi rendszerhez egy veszélyt jelentő rendszernek, új shellt indított a TCP 4444-es portján és letöltötte a féreg maradék részét az UDP 67-es porton TFTP-t használva. A trójai újrakreálta magát egy msblaster.exe nevű fájlban, ami bekerült a registry egyik automatikusan elinduló helyei közé. A vírus újraindította a számítógépet és elkezdte használni a frissen megszerzett hostot, hogy más gépeket is megfertőzzön.

Amikor a Blastert először jelentették, sok szervezet lassan reagált, mivel széles körökben azt hitték, hogy a megfelelően konfigurált kerületi tűzfal, ami nem engedélyezi a TCP 135-ös portján a bejövő forgalmat, meg fogja állítani a Blaster fertőzéseit a helyi számítógépeken. De aztán fertőzött gépek csatlakoztak a közös hálózatba VPN-eken keresztül valamint már előzőleg fertőzött laptopok is csatlakoztak a "védett" közös hálózatba, kirobbantva a Blastert a biztonsági frissítésekkel még nem rendelkező hálózatbeli gépek sokaságán. Egy fertőzött számítógép gyorsan tovább terjesztette a férget a hálózat sebezhető gépeit. A Blaster sebezhető gépek százainak, ezreinek megfertőzéséért felelős órákon belül. A helyrehozó folyamatokat tovább nehezítette, hogy egy ehhez kapcsolódó, Nachi névre hallgató féreg lett kifejlesztve pár napon belül, ami egy félrevezető frissítési merénylet volt a gyenge gépek ellen. A terv szerint megfertőzi a sebezhető számítógépeket, hasonló módon, mint ahogy a Blaster tette, és azután kísérletet tesz a Blaster fertőzéseit meggátoló biztonsági frissítés telepítésére. Szerencsétlenségükre a Nachi lett a példája annak, hogy miért nem szabad automatizált malware-t használni a számítógépes problémák megoldására, a számítógép birtokosának beleegyezése nélkül. A Nachi alapvetően arra utasította a hálózat gyenge gépeit, hogy töltsenek le egy biztonsági frissítést, mind egyszerre, elnyomva ezzel a hálózati erőforrásokat. Amikor feltelepítette a frissítést, teljesen hibásan, gyakran abban az állapotban hagyta a rendszert, hogy védelmezi a sebezhetőket. A Nachi végül több problémáért és üzemszünetért volt felelős, mint a Blaster vírus.

A Microsoft a Blaster után jelentős változtatásokat hajtott végre a műveleteiben, agresszívvá tette a kitakarítást és automatizálta a biztonsági frissítéseket a számítógépekre. Habár a Windows felhasználók már régóta használták a Windows Update-et és egyéb frissítést letöltő klienseket (a Windows 98 óta), a Microsoft még több automatán frissítő szolgáltatást fejlesztett ki, beleértve a korábbi Automatikus Frissítések javított változatát, és bejelentett egy ingyenes szoftverfrissítési szolgáltatást / Windows szerver frissítési szolgáltatást (SUS/WSUS) cégeknek, amik nem használtak egyéb patch kezelési szolgáltatást. A Microsoft továbbá megkönnyítette az új operációs rendszer telepítésekor, hogy egyúttal a frissítések is letöltésre kerüljenek, a hálózati kitettség kockázatának minimálisra csökkentésével, oly módon, hogy lecsökkentette a hálózati eléréseket mindaddig, amíg a frissítések fel nem települtek. A Blaster legnagyobb tanulsága a számítógép biztonságának elemzői számára az volt, hogy a kerületen elhelyezett tűzfal védelme nem elegendő. A Windows XP 2-es szervizcsomag (SP2) és későbbi Windows kliens gépek óta a host-alapú Windows tűzfal van engedélyezve alapértelmezettként. Ez az egyszerű intézkedés számítógépek millióinak megvédéséért felelős a számos távoli rosszindulatú támadások veszélyeztetésétől.

A gyakori szolgáltatás támadások és sebezhetőségek

Minden egyes telepített és aktívan működő szolgáltatás egy sebezhető pont a rosszindulatú hackereknek.

Puffer túlcsordulás

A szolgáltatások közül majdnem mindegyikhez tartozik egy bejövő forgalmat hallgató csatorna a távoli elérések miatt. A puffer túlcsordulás akkor keletkezik, amikor egy szolgáltatás input rutinja több információt engedélyez elküldésre, mint amennyire korábban be lett állítva a puffer tartaléka. A sebezhető szolgáltatásokat ki lehet használni, hogy szétbomlasszuk, vagy ami még rosszabb, a támadónak jogot adjunk belépni a rendszerbe a service log-on accountjával. Ha ez egy helyi rendszer vagy egy adminisztrátor, a támadók bármilyen műveletet elvégezhetnek, irányíthatják a rendszert, letölthetnek és telepíthetnek még több malware-t, vagy betölthetnek shelleket távoli irányítás céljából.

Távoli bejelentkezésű hozzáférés

Sok szolgáltatásnak (FTP, IIS, Remote Desktop, terminálszolgáltatások, stb.) van bejelentkezési pontja, ahova egy behatoló megpróbálhat illetéktelenül betörni azzal, hogy próbálkozik a név és jelszó beírásával. Alaphelyzetben az adminisztrátori fiókot nem lehet zárolni a fiókszáróási beállítások szerint. A betolakodóknak módjukban áll automatizált jelszótörő programot használni vagy manuálisan újra és újra próbálkozni. Amíg a biztonsági naplót nem ellenőrzik a hibás bejelentkezések után kutatva, a jelszó kitalálást elég sok ideig lehet észrevétlenül csinálni.

Hallgatózás / szimatolás

Mivel minden szolgáltatás ami bejövő adatokra vár (hallgatózik), az fogad és küld is adatokat, a támadók ezeket a beszélgetéseket elfoghatják, az adatokból illetéktelen információhoz juthatnak. Sok szolgáltatás (SNMP, Telnet, FTP, POP, stb.) használ sima szöveg alapú bejelentkezési nevet és jelszót. De még egyéb, nem sima szöveget használó alkalmazásokat is ki lehet használni. Példaként a már javított RDP szolgáltatást lehet említeni, amit megjelenése után rögtön támadás ért annak ellenére, hogy titkosítást használt. Egy új munkamenetet elkaptak és átirányítottak a támadón keresztül. Mivel az RDP nem autentikálta a végponton a klienst, egészen a 6.0-s verzióig, lehetséges volt, habár különösen nehéz a támadók számára, hogy bekerüljenek a kommunikáció adatfolyamába és kizsedjék a titkosított jelszókat, egy karaktert egyszerre. Számos hackelésre szolgáló eszköz valósította meg az RDP támadását, olyan egyszerűen, hogy csak pár kattintás kelljen hozzá és átjuttatja a támadót a kommunikációs útba való becsöppenés jelentős akadályain. A szimatolást szintén arra lehet használni, hogy bizalmas és személyes információra tegyünk szert a bejelentkezési igazolást kikerülve.

Jelszó fenyegetettség

Teljesen veszélyeztetett rendszerek további hálózati jogok kiterjesztéshez vezetnek, használva a felsorolt jelszavakat a service log-on accountokból. Ha egy támadónak

feljogosított belépése van (mint egy adminisztrátornak, vagy helyi rendszer esetén) a rendszerbe, akkor számos módszer és eszköz áll a rendelkezésére, hogy visszafejtsen biztonsági igazolásokat egy service log-on accountról sima szövegben. Ha a visszafejtett igazolásokat más gépeken, vagy a tartománybeli helyeken használni tudjuk, akkor ezenfelül engedélyezni fogják az erőforrások veszélyeztetését is.

Rosszul beállítás

Egy szolgáltatás lehet megfelelően lekódolva és nem kell hogy bármilyen ismert gyengeséget tartalmazzon, még mindig ki van téve a rosszindulatú használatnak. Gyakori, hogy a felhasználók vagy adminisztrátorok rosszul állítsanak be szolgáltatásokat, ezzel megnyitva az utat az illetéktelen behatolásoknak. Például: egy felhasználó telepít IIS vagy FTP szolgáltatást, de gyenge jelszót használ. Vagy a felhasználó egy elosztott hálózati alkalmazást telepít, azzal a céllal, hogy kisebb könyvtárakat osszon meg, helyett megosztja az egész merevlemezt. Az utóbbi probléma már számtalanszor fordult elő, bizalmas és top-secret dokumentumok kerültek véletlenül napvilágra az interneten.

Társadalomra tervezve

Szolgáltatások, amelyek aktívan kommunikálnak a végfelhasználókkal, mint például az elosztott fájlmegosztó rendszerek, egy újabb lehetőséget kínálnak a malware terjesztőknek, hogy kijátsszák a felhasználókat és azok futtassák a programjaikat. Egy peer-to-peer (P2P) malware meghamisíthat egy beszélgetést a felhasználóval és küldhet egy elfogadási kérelmet, hogy az fogadjon el egy fájl átvitelt. A fájlátvitel úgy van hirdelve, hogy az valamilyen legitim tartalommal bír, helyett egy trójai malware-t tartalmaz. Ezenfelül a legtöbb anti-malware program nem ellenőrzi a szolgáltatások bejövő tartalmát, gyakorlatilag engedélyezve ezzel, hogy megfertőződjön a gép, még akkor is, ha elvileg védett. A szolgáltatások kifejezett célpontjai sok különböző formájú rosszindulatú támadásnak, és minden egyes futó szolgáltatás növeli a veszélynek kitettség kockázatát.

Szolgáltatás erősítés

A Blaster vírus után a Microsoft fenyegetettség alapján lemodellezte az alap Windows szolgáltatásokat, hogy megnézzék és csökkentsék a biztonsági kitettségüket. Ez az erőfeszítés megváltoztatta az alapértelmezett felhatalmazásokat és jogokat, valamint sok új szolgáltatással kapcsolatos biztonsági intézkedés megtételéhez vezetett. Tehát a Windows Vista és későbbi verziók alatt futó szolgáltatások számos új fejlesztést tartalmaznak a korábbi Windows kliensek alatt futókkal szemben, beleértve:

- Minden szolgáltatásnak egy legkisebb jogú modellje van
- A szolgáltatások szét lettek bontva, így több szolgáltatás fut a Helyi szolgáltatás vagy Hálózati szolgáltatás log-on környezetében
- Minden szolgáltatás rendelkezik egy biztonsági azonosítóval (SID), hogy szolgáltatásonként irányítsuk az engedélyeket
- Lektorlátozott SID-ek tartoznak egy pár szolgáltatáshoz
- Szolgáltatásokat lehet lekorlátozni a hálózati tartománnyal
- A 0. munkamenet izolációja minden Windows szolgáltatás számára szükséges
- Adatvégrehajtás megelőzés be van kapcsolva a szolgáltatásoknak
- Ellátási lánc menedzsment (SCM) állapot bejelentése javult

A Windows Server 2008 (és Windows Vista) alatt futó szolgáltatások jelentősen javultak az előző Windows verziókhoz képest. A legkisebb jogú módban futnak, szolgáltatás-specifikus SID-del, 0. munkamenetben izolálva, korlátozott hálózati hozzáféréssel, DEP és ASLR védelemmel. Az adminisztrátorok segíthetik a szolgáltatások rosszindulatú kitettség kockázatának csökkentését a szükségtelen szolgáltatások környezetből való eltávolításával, és követik a legkisebb jogú modellt a szolgáltatásokkal, amiket terveznek és megvesznek. Habár a Windows mindig is egy célpont lesz a rosszindulatú hackereknek, ezek a szolgáltatások már keményebbé teszik a siker elérését számukra.

Csoportházi rend

A Csoportházi rend (Group Policy) technológia a Windows 2000 óta használatos. Ez a multifunkciós konfiguráció technológia a Windows szerveren és az asztali operációs rendszereken belül. A technológia arra lett tervezve, hogy központilag konfiguráljunk szó szerint beállítások ezreit, amik valamennyi vagy minden Windows rendszerünkre vonatkoznak a különböző hálózatokban. A Group Policy a kulcs mechanizmus a biztonsági beállítások felvonultatására minden rendszerünkben. Ha másra nem is, a legtöbbben már használták a csoportházi rendet a jelszóházi rend beállítására az Active Directory tartományban.

Mi új a Windows Server 2008 csoportházi rendjében

A Windows Server 2008 és Windows Vista jó pár jelentős javítást jelentett be, amelyek a Windows XP és Windows Server 2003 óta történtek. Valójában a legtöbb ezen változtatások közül először a Windows Vista alá lett bejelentve, azután onnan öröklődtek tovább a Windows Server 2008 alá. Ezt leszámítva a Windows Server 2008-nak megvannak a maga változtatásai – főként a Group Policy Management konzollal kapcsolatosak (GPMC) – amik további kezelhetőséget biztosítanak a csoportházi rendnek.

A kulcs változtatások amelyeket bejelentettek a Windows Server 2008 és Windows Vista alá:

- Több házi rendet támogat, beleértve az új vezetékes és vezeték nélküli hálózatok biztonságának házi rendjeit, javított Windows tűzfal és IPsec házi rend konfigurációs interfészek, áramellátás menedzsment konfiguráció és USB készülék korlátozás házi rendek.
- Javított slow-link felismerés a kliens és a DC között. Megbízhatóbb mechanizmus annak meghatározására, ha a kliens slow-linken keresztül. Ez kihathat a csoportházi rend feldolgozó magatartására.
- A Group Policy frissítése a DC elérhetőségén alapszik egy rögzített ciklus helyett. Ez azt jelenti, hogy ha egy kliens visszacsatlakozik a közös hálózatba vagy távolról VPN-en keresztül csatlakozik, akkor a Group Policy gyakrabban frissül.

- Támogatás a többszörös Local Group Policy Object-eknek (LGPO), felhasználói, adminisztratív és nonadminisztratív szűrés engedélyezésére a helyi csoportházirendben.
- Támogatás az új XML alapú Adminisztratív Minta fájltypusnak (Administrative Template file format, ADMX), ami javítja a többnyelvűséget az adminisztratív minták számára.
- Fejlesztések a GPMC és csoportházirend szerkesztő számára a Windows Server 2008-ban, ami új lehetőségeket tár elénk, mind például a házirendek szűrése amik kulcsszavak alapján jelennek meg, és a képesség, hogy csináljon "kezdeti" GPO-kat az adminisztratív minta házirend számára.
- A Group Policy Preferences újítás, ami összeolvasztja az új házirend beállításokat, amik korábban a DesktopStandard PolicyMaker technológia részei voltak, amiket a Microsoft szerzett.

Csoportházirend szolgáltatás

Az első változás a Group Policy infrastruktúrájában többé-kevésbé láthatatlan volt az adminisztrátorok számára. A Windows Vista és Windows Server 2008 előtt, a Group Policy motorja a megbízható Windows szolgáltatás, a Winlogonban futott. Ennek volt valamennyi értelme abban az időben, de kihívásokkal is szolgált. Microsoft vagy third-party (harmadik féltől származó) Kliens oldali kiterjesztések (CSE) szintén futottak ezen a folyamaton belül, és ha valamilyen bug keletkezett a futás során, az azt okozhatta, hogy a Windows nem válaszolt. A Microsoft a Windows Vistában és Windows Server 2008-ban kivette a Group Policy motorját a Winlogonból és beletette a Group Policy kliens szolgáltatásba, ami a svchost.exe-ben fut, eltekintve attól, hogy azt nem tudják elindítani vagy leállítani az adminisztrátorok (legalább is nem olyan egyszerűen). Mivel a szolgáltatás nem a Winlogonban fut többé, ezért egy hibás CSE nem fogja lefagyasztani a teljes operációs rendszert.

Összefoglalás

A Windows Server 2008 új vonásai nagyon fontosak. Annak a megértése, hogy hol történtek változtatások, de ha nem változtatások, akkor javítások, segít abban, hogy megértsük, hogyan is működik ez a technológia. A tudás birtokában lenni, hogy milyen hardware elemek a megfelelőek és mely operációs rendszerek milyen feladatra, milyen funkcionalitásra vannak tervezve, kritikus, ha új szerver választására kerül a sor, vagy ha fel kell mérni, hogy egy létező szerver készen áll-e ezen feladatok ellátására. A kulcs jellemvonások ismerete növeli a felhasználó tapasztalatát, az adminisztrátor tapasztalatát, a szervezet biztonságát.

Habár csak pár lényeges dolog került említésre, a Windows Server 2008 ennél jóval többet tartalmaz. A Microsoft munkatársai nem sajnálták az időt és pénzt beleölni a fejlesztésbe, ha a biztonság a tét. Hackerek mindig is vannak, voltak, lesznek, a hosszú távú célkitűzés azonban az, hogy egyre kevesebb helyen vagy egyáltalán ne tudjanak betörni a rendszerünkbe.

Irodalomjegyzék

Microsoft Press Windows Server 2008 Security Resource Kit eBook

Windows Server 2008 Networking and Network Access Protection eBook

Securing Windows Server 2008 Prevent Attacks eBook

http://www.microsoft.com/hun/ws2008/longhorn_overview.mspx 2009.03.21.

http://en.wikipedia.org/wiki/Computer_security 2009.04.17.

http://hu.wikipedia.org/wiki/Windows_Server_2008 2009.04.17.