A Windows 2000 biztonságos üzemeltetése[1]

Ez a fejezet azt a célt tűzte ki, hogy segítse a kezdő- illetve középhaladó rendszergazdákat, hogy a Windows 2000 alapú hálózatát minél biztonságosabbá, használhatóbbá tegyék.

A probléma

Biztonság kontra használhatóság

Sajnos, nagy általánosságban kijelenthetjük, hogy ez a két fogalom a számítógépes hálózatok esetén egymással ellentétes, fordított arányban áll. A rendszergazda minél biztonságosabb (stabilabb, nehezebben elrontható, elkonfigurálható, beavatkozás-mentes) hálózat iránti igénye ugyanis csak a felhasználók szabadságának (jelen esetben jogosultságainak) korlátozásával valósítható meg. A rendszergazda általános törekvése *a mindenkinek csak a feltétlen szükséges jogosultság* érthető nézőpont, hiszen csökkenti mind a szándékos, mind a véletlenszerű, a rendszer szempontjából romboló jellegű műveleteket.

Abban az esetben, ha mondjuk tiltjuk a törlési és létrehozási jogokat, akkor a felhasználót esetleg akadályozhatjuk a munkájában, ha az adott dokumentumot szánt szándékkal törölni szeretné, vagy új dokumentumot szeretne létrehozni. Viszont ha a felhasználók számára maximálisan használhatóvá kívánjuk tenni a gépeket, ezzel „kiskapukat" nyitunk az esetlegesen ártó (jórészt nem szándékos) műveleteknek.

Mi tehát a megoldás, hogyan konfiguráljunk egy hálózatot? Ez egy nagy kihívás, és erre nem is lehet általános „receptet" adni, de ebben a fejezetben megtalálható pár irányelv, illetve szükséges módszer ismertetése, mely segítségével egy kompromisszumos megoldás kidolgozható.

A főbb veszélyforrások

Egy számítógépes hálózat biztonságát (akár az érzékeny állományok védelméről, akár a szolgáltatások, illetve a hálózat üzembiztosságáról van szó) több tényező befolyásolja, ezeket két fő csoportba sorolhatjuk: a belső (hálózaton belülről érkező), illetve a külső (kívülről pl. Internetről érkező) veszélyforrá-

[1] Részlet Holczer-Benkovics: A Windows 2000 Server üzemeltetése – Internet és Intranet c. könyvünkből. (Jedlik Oktatási Stúdió, Budapest, 2002. (Rakt. sz:. JO-0007)

sokra. Tekintsük át az alábbi táblázatot, mely egy amerikai statisztikai forrásból származik.

1.	Visszaélés a meglévő jogosultságokkal	43%
2.	Belső felhasználók jogosulatlan hozzáférése	22%
3.	Denial of Service támadások	14%
4.	Külső hálózati támadások	13%
5.	Szabotázs	8%

A fenti táblázatból jól látszik, hogy a problémák közel 2/3-a (65%) hálózaton belüli. Az első lépéseknek ezek kivédésére kell irányulniuk.

A támadók eszköztára

Cracker - jelszófeltörő

A jelszófeltörő egy olyan program, amelynek célja az, hogy segítségével „visszafejthessük", hozzájuthassunk például a rendszergazdai jelszóhoz. Régebben egy ilyen program írása komoly programozói és rendszerismereteket követelt, de manapság ezek a programok az Internetről is letölthetők. Ilyen például a *lopthcrack* program.

A jelszó feltörése tulajdonképpen NT és 2000 esetén inkább próbálkozásos elvű, ún. *brute-force* módszer. Ennek oka az, hogy a jelszó ténylegesen visszafejthetetlen, ugyanis maga a jelszó nem tárolódik le, csak valamilyen HASH tördelőalgoritmusos kivonata.

A *HASH tördelőalgoritmusok* alapelve az, hogy veszek egy szöveget (pl. a jelszó), és ebből készítek egy olyan egyedi fix hosszúságú kivonatot, mely egyértelműen azonosítja a szöveget. Magából a kivonatból már az eredeti szöveg nem nyerhető vissza, de ugyanazt a szöveget az algoritmuson még egyszer áteresztve ugyanazt a kivonatot kapom. Magát a kivonatot úgy kell elképzelni, mint a sertést és a fasírtot. A sertésből előállítható a fasírt, mely egyértelműen azonosítható, mint sertés fasírt, egy másik sertéssel a műveletet elvégezve a végeredmény azonos lesz, de a fasírtból már soha nem nyerhetjük vissza a sertést.

A fentiek alapján tehát a törőprogram nem csinál mást, csak végigpróbálja a betűkombinációkat, mindegyikből előállítja a kivonatot, és összehasonlítja az eredeti, tárolt jelszókivonattal. Ha a két kivonat stimmel, megvan a jelszó. Egyes programoknak megadhatunk egy szótárt is, mely segítségével előbb végigpróbálja a szavakat, csak utána kezdi a hosszadalmas betűkombinálást.

Érdemes tudni, hogy az ilyen jelszófeltörések ellen az NT4-ben a HiSec csomaggal védekezhettünk, míg a Windows 2000 már alapból is jóval védettebb.

Sniffer - forgalomelemző

A forgalomelemző általában valamely hálózat-felügyeleti program része (például a Windows-os *Network Monitorban* is van). Alapvető célja a hálózati forgalom figyelése, és az esetleges jelszók, azonosítási információk elcsípése.

Backdoor – hátsó bejárat

Ez egy elnevezés arra, hogy a programban eredetileg is meglévő gyengeségek kihasználásával juthatunk át biztonsági réseken. Ehhez mindig ismerni kell a megcélzott operációs rendszert, hiszen a hiba rendszerfüggő. Ilyen hiba volt például a NT4-ben az, hogy a szerver közvetlen hozzáférésével (ez eleve hiba, mivel a szerver(eke)t fizikailag is érdemes elzárva tartani) valamilyen módon sikerül kitörölnünk a fájlt, amely a SAM (*Security Accounts Manager*) adatbázist tartalmazza, a következő indításkor a rendszer új adatbázist hoz létre, ÜRES adminisztrátori jelszóval.

Buffer Overrun – veremtúlcsordítás

Ez a módszer szintén egy adott alkalmazás hibáját használja ki, egy adott függvény hibáján alapul. Alapvető célja, hogy a vezérlést átvéve, rendszerjogokkal elindíttatunk egy saját programot. Az eljárás tömören: valamely beviteli ponton a függvényt túlcsordítjuk, és a megfelelő helyre beszúrva egy memóriacímet, „elugrattathatjuk" oda a rendszert, és ott folytatja a végrehajtást. Ez a módszer komoly programozási ismereteket feltételez.

Denail Of Service – szolgáltatás-megtagadás

Az eljárás célja egy szolgáltatás túlterhelése, ezáltal rendszerösszeomlás elérése. Ennek két célja lehet: pusztán bosszúságot okozni, illetve egy jóval alattomosabb, újraindítást kieszközölni, melynek esetleges haszna, hogy a más eszközökkel elért módosítások érvényre juttatása.

Trojan – trójai faló

Mint a neve is mutatja, ez egy olyan ártalmatlannak kinéző kis programocska, ami abszolút nem az, aminek látszik. Ilyen például a *Back Orifice* „távmenedzselő" eszköz, mellyel rengeteg bosszúság okozható a mit sem sejtő rendszergazdának.

Védekezési alapelvek

Nézzünk néhány alapelvet, melyet érdemes betartani a hálózatunk védelme érdekében:

A legkisebb szolgáltatás elve: Általános szabály, hogy minél több a szolgáltatás, minél több a kapu, annál több a lehetséges bejárat, hátsó kapu.

Az ismeretlenség biztonsága: Ha nem tudják mit (milyen operációs rendszert, milyen nevű gépet, milyen típusú szolgáltatást) lehet támadni, akkor nem tudják helyből, hogy mely eszközöket kell bevetni.

A leggyengébb láncszem: az ember: Sajnos a fontos termékfrissítések nem képesek „maguktól" települni, ezért nagyon fontos, hogy a rendszergazda tudjon a szükséges módosításokról, és telepítse azokat.

Rendszerelemek

A szerver(ek)

Az egyik legfontosabb szempont a szerver operációs rendszerének (Windows 2000 Server) megfelelő konfigurálása, védelme. Hiszen a server/client hálózatok esetén a szerver(ek) központi, kiemelt helyen szerepelnek, biztosítják az adatokat, felhasználásokat a munkaállomások számára, éppen ezért nagyon fontos, hogy ezek a gépek mind szoftver, mind hardver szintjén megfelelően védve legyenek.

Ami a szoftveres védelmet illeti, magának az operációs rendszernek a védelme sokat javult az NT4 óta, ami azt jelenti, hogy egy újonnan felhúzott szerver alapból sokkal hatékonyabban védi magát a hálózati operációs rendszert is. Itt érdemes pár szót ejteni a szerver hardveréről, illetve a hardver megfelelő védelméről: A jó minőségű hardver elsősorban az üzembiztosság, és a rendelkezésre állás szempontjából érdekes. Nagyon fontos viszont, hogy a szerver „vasat" – magát a gépet – megfelelően „lakat alatt tartsuk" a szó szoros értelmében, azaz lehetőség szerint zárható, külön helységben helyezzük el, ezáltal is csökkentve a közvetlen támadások (ha valaki közvetlenül – nem hálózaton keresztül – hozzáférhet a szerver gépekhez) esélyét.

A munkaállomások

A munkaállomások biztonsági beállításai, stabilitása alapvetően befolyásolhatja a hálózat stabilitását, mivel a felhasználó munkaállomások előtt ül. Hiába van egy stabil, jól beállított hozzáférési jogosultságlistánk a szerveren, ha a munkaállomáson a felhasználó letörli a Windows rendszerállományait, és a gép nem tud elindulni. Abban az esetben, ha a munkaállomásokon is Windows 2000-et (Windows 2000 Professional) használunk, szintén sokat profitálunk az új operációs rendszer megnövelt „önvédelmi" képességéből.

Természetesen a hálózat tagjai lehetnek más operációs rendszerrel rendelkező gépek is, de ebben az esetben a helyi biztonság csorbát szenvedhet. Ennek

oka a két operációs rendszer család (az *otthoni* Windows: 95,98,Me, és az *üzleti* Windows: NT, 2000) közötti különbség:

Windows 9x/Me és a Windows NT/2000 közötti különbségek

A két operációs rendszer-család (Win95/98 és WinNT/2000) annak ellenére, hogy felhasználói felületük közel azonos, lényegi különbségeket hordoz magában. Ezek a szerkezeti, felépítési különbségek határozzák meg a két operációs rendszer javasolt felhasználói területeit.

A *Windows NT család* (Windows NT 4.0, valamint a jelenlegi Windows 2000 család) alapvető rendeltetése a *nagyfokú biztonság* (felhasználói adatok védelme), a többfelhasználós és hálózati működés valamint a stabilitás. Ezt az operációs rendszer úgy éri el, hogy nem engedi meg az alkalmazások számára (Word, játékok, stb.), hogy közvetlen módon hozzáférhessenek a számítógép erőforrásaihoz. Ez rendkívül fontos, hiszen statisztikák alapján a rendszerfagyások nagy százalékának oka az, hogy egy adott alkalmazás nem megfelelő módon kezeli a számítógép erőforrásait, ezáltal más alkalmazásokkal vagy magával az operációs rendszerrel is összeakadhat. Sajnos ennek a rendszernek van hátránya is. Mivel a rendszer (Windows NT) nem engedélyezi a közvetlen hardverhozzáférést, ezért néhány játék vagy multimédiás alkalmazás nem (vagy nem megfelelően) fut. Bár ez a kijelentés szerencsére elsősorban az NT4 Workstation operációs rendszer esetén igaz, a 2000 Professional sokkal nagyobb körű – szinte a Windows 98/Me-vel azonos, néhány területen azt is túlszárnyaló – játék, és multimédia támogatással rendelkezik.

Egy másik fontos szempont a *hardverigény*. A Windows NT/2000 családnak nagyobb a hardverigénye (azaz ugyanolyan gépen kisebb teljesítménnyel fut, mint a Windows 9x), illetve az NT4-nek kisebb a hardver kompatibilitása is, azaz nem támogatja az összes piacon lévő hardvert. Szerencsére mostanában az összes újabb hardver már Windows NT-s meghajtó-programokkal (driver) kerül forgalomba, mely lehetővé teszi az eszköz Windows NT alá illesztését. Windows 2000 Professional alatt óriási gyári driver adatbázis áll rendelkezésünkre, szinte minden, manapság használatos és divatos hardvert alapból ismer.

A *Windows 9x család* (Windows 95/98/Me) elsődlegesen otthoni felhasználásra készült, célja a számítógép erőforrásainak maximális kihasználása, maximális multimédia és játéktámogatás. Ezek az operációs rendszerek nagyfokú hardver kompatibilitással rendelkeznek, lehetővé válik „speciális” hardverek használata is. A multimédiás alkalmazások és a játékok közvetlenül használhatják a hardver eszközöket, ezáltal gyorsabb futást, megjelenítést tesznek lehetővé. Viszont ebben az esetben, ha egy adott játék megfagy, az általában magával rántja a teljes rendszert. Egy másik előnye a Windows 9x rendszereknek az NT-vel szemben, hogy támogatja a PnP (*Plug And Play*) eszközöket. Természetesen a Windows 2000 család már szintén PnP.

Egy további rendkívül fontos szempont: a Windows 9x csak a FAT vagy a FAT32 fájlrendszereket ismeri, mely *nem támogatja a fájlrendszer szintű védelmet*, azaz a munkaállomáson lévő állományok hozzáférési jogosultságait nem szabályozhatom, bárki letörölheti az állományokat, így lehetetlenné téve a munkaállomáson a Windows elindulását. Ha azonban a munkaállomásainkon Windows NT/2000-t futtatunk, és azt NTFS-re telepítjük, lehetővé válik a lokális állományok védelme is, így nem törölhetők le jogosulatlanul vagy véletlenül a rendszerfájlok.

*Összefoglalva:*A Windows 9x családnak jobb a hardver, multimédia és játéktámogatása, mint a Windows NT családnak, viszont cserébe kisebb a rendszer stabilitása, könnyebben tönkretehető és kevésbé támogatja a hálózati működést. Abban az esetben, ha lehetőségünk van munkaállomás oldalon is a Windows 2000-et választanunk, az ideális megoldás, mely ötvözi a Windows 9x multimédia, PnP támogatását az NT stabilitásával.

A központi felügyelet (Active Directory)

Egy tisztán Windows 2000-es rendszerben (ahol mind a szerver, mind a munkaállomások Windows 2000-et futtatnak) nagyon sokat fejlődött a központi rendszerfelügyelet. A szükséges változtatásokat, beállításokat a rendszergazda egy gép elől elvégezheti, nem kell odamennie a munkaállomásokhoz sem. Például lehetőségünk van központosított szoftvertelepítésre is, azaz egy adminisztrációs gép mellett ülve úgy telepíthetjük az Office 2000-et egy tetszőleges munkaállomásra (vagy azok csoportjára), hogy nem kell a felhasználónak beavatkoznia, csak újra kell indítania a gépet, a telepítés önműködően lezajlik. Ugyanígy lehetőségünk van immár az összes munkaállomásunk helyi biztonsági házirendjének (mely szabályozza az adott munkaállomás helyi biztonsági funkcióit, beállításait) központi ellenőrzésére, sőt beállítására is.

Kerberos

Beléptetés, hitelesítés

Ahhoz, hogy egy felhasználó használni tudja a hálózatot, be kell lépnie, azaz a rendszernek hitelesítenie kell a munkaállomáson ülő embert. A hitelesítés - amely természetesen titkosítva zajlik – folyamata a következő: a munkaállomás egy hitelesítési kérelmet küld a hálózatra (jelzi, hogy egy adott felhasználó be kíván lépni), a kérelemre az első elérhető tartományvezérlő válaszol (hogy melyik, az például a terheltség függvénye). A beírt felhasználói név és a jelszó

alapján, ha az egyezik a hitelesítő szerver felhasználói adatbázisával a felhasználó megkapja az ún. *access tokent*.

Tisztán 2000-es hálózatban a *Kerberos hitelesítési protokol* lép üzembe, mely sok korábbi hiányosságot és rugalmatlanságot megold. Mivel ez a rendszer „jegy" alapú szolgáltatás (a felhasználó belépésekor egy TGT-t (*Ticket Granting Ticketet*) kap, mely definiálja, hogy milyen típusú további szakaszjegyeket kérhet a különböző erőforrások eléréséhez). A jegynek érvényességi ideje van, ezért egy esetleges csoporttagság váltás esetén a felhasználónak nem kell újra belépnie, hanem egy adott idő után a változtatások érvényre jutnak.

Kerberos

A Kerberos tehát a Windows 2000 alapértelmezett hitelesítési protokollja. Lehetővé teszi, hogy egy felhasználó egyszeri belépéssel a hálózat összes gépéhez, a megfelelő jogosultságokkal, hozzáférhessen. Ennek a megvalósítása a szerver oldali komponensek (Kerberos szolgáltatás a tartományvezérlőkön), illetve kliens oldali komponensek (a Windows 2000 munkaállomásokon) együttműködésével válik lehetővé.

Fontos, hogy ha Windows 9x klienseket is használunk, a Kerberos kliens oldali komponenseit az Active Directory kliensszoftverrel telepíthetjük fel. A megfelelő kliens szoftver nélkül ezek az operációs rendszerek az NTLM hitelesítési eljárást használják.

A rendszer működésének kulcsa a központosított kulcskezelés, melyet a *Kerberos Key Distribution Center* (KDC) végez el. A felhasználó, mielőtt elérné az adott erőforrást egy szerveren kér egy ún. *szakaszjegyet* erre a szerverre a KDC-től, és ezt a jegyet küldi el a célszervernek. Fontos, hogy a szakaszjegynek lejárati ideje van. Ha a jegy lejárt egy aktív kapcsolat közben, a KDC frissíti a jegyet, és ezt elküldi az érintett kliensnek és a szervernek is. Ez fontos előny, hiszen így kivédhetők az olyan problémák, miszerint ha egy felhasználó belépett, akkor hiába váltom a csoporttagságát, vagy akár hiába törlöm a felhasználót, amíg ki nem lép, a belépéskori jogait élvezi. Mivel a jegyeket frissíteni kell, így a frissítéskor érvényre juthatnak a megfelelő változtatások.

Egy nagy előnye a Kerberos használatának a *jegytovábbítás* lehetősége. Ez akkor válhat szükségessé, ha a felhasználó csatlakozik egy adott szerverre, de annak a szervernek egy további szerverről kell adatokat kapnia, az eredeti felhasználó jogkörével. Ekkor a rendszer lehetőséget biztosít arra, hogy az elsődleges szerver jegyet kérjen a másodlagos szerverre a felhasználó jogkörével.

Új eszközök a biztonsági beállításokra

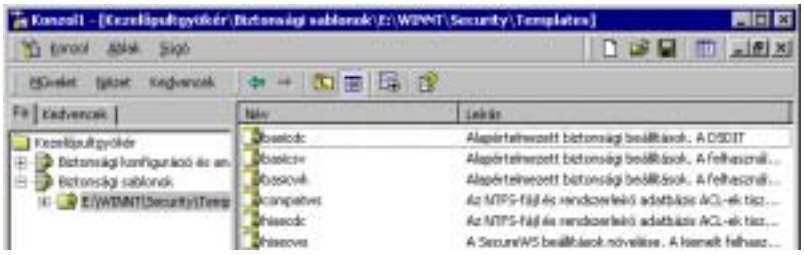
Biztonsági konfiguráció és analízis

Ez az eszköz lehetőséget ad arra, hogy a hálózatunk Windows 2000-es gépeinek helyi biztonságát beállítsuk, illetve felügyeljük. Ezek a beállítások kiterjedhetnek a számítógép biztonsági beállításaira, de a fájl szintű jogosultságokra is. Vegyünk egy példát: egy nyilvántartó programot kell telepítenünk, melynek olyan komponensei vannak, amelyeket a helyi gépre kell telepíteni. A program telepítését elvégeztük, de szeretnénk, hogy a gépeken szereplő programkomponensek (amelyek csak a rendszer töltődését végzik el) ne válhassanak véletlen, vagy szándékos törlés „áldozataivá". Erre a megoldás természetesen az, hogy fájl szinten, a hozzáférési jogosultságokat módosítjuk (pl. a programhoz tartozó könyvtárakra csak olvasási jogot adunk az átlagfelhasználóknak). Normális esetben ezt minden gépen helyileg meg kéne tenni. Ha ezt nem így kívánjuk megtenni, két módszerünk van.

Az egyik lehetőség, minden gépen helyileg lefuttatni azt a biztonsági konfigurációs sablont, melyen létrehozásnál beállítottuk a kért fájl-hozzáférési változtatásokat. A másik az, hogy az Active Directory-ban hozzáadjuk az adott gépeket magába foglaló szervezeti egységhez a sablont, és újraindíttatjuk az érintett gépeket.

A sablonokat, illetve az azokat kezelő programfelületet a következő módon érhetjük el. A Start menüből válasszuk a *Futtatás* menüpontot, majd írjuk be *MMC*. Ezzel elindítottuk a *Microsoft Management Consolt*, azt az egységesített keretprogramot, melyet a Windows 2000 adminisztrációs eszközei használnak.

Miután bejött a program, válasszuk a *Konzol* menü *Beépülő modul hozzáadása/eltávolítása* menüpontot. A megjelenő ablakban válasszuk a *Hozzáadás* gombot, majd adjuk hozzá a *Biztonsági konfiguráció és analízis* valamint a *Biztonsági sablonok* elemeket a *Hozzáadás* gomb segítségével, végül zárjuk be az ablakot, és *OK* a beépülő modul hozzáadása ablakon.



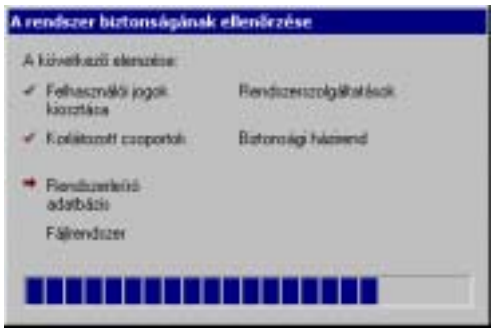
Visszatérve az *MMC* ablakára láthatjuk, hogy az adminisztrációs felületünkön megjelent a két kiválasztott modul. Az első (*Biztonsági konfiguráció és analízis*) az eszköz, mellyel leellenőrizhetjük illetve felkonfigurálhatjuk, hogy a

rendszerünk mennyiben egyezik egy általunk megadott adatbázissal, mely különböző biztonsági értékeket definiál. A második (*Biztonsági sablonok*) néhány, előre elkészített sablont tartalmaz. A nevek mellett rövid leírást is találunk az adott sablonra vonatkozóan.

Nézzük, hogyan használhatjuk ezen eszközöket. Tételezzük fel, hogy szeretnénk az egyik munkaállomásunkat (amely alapból, NTFS-re történő telepítés esetén a *Setup Security* sablon alapján jön létre) nagybiztonságú munkaállomássá (*Hisecws sablon*) tenni.

Elsőként létre kell hoznunk az adatbázist, amely a szükséges módosításokat hordozza magában. Kattintsunk jobb gombbal a *Biztonsági konfiguráció és analízis* modulon, majd válasszuk az *Adatbázis megnyitása* funkciót. Ezután adjunk valami nevet az adatbázisunknak (pl. Hisec) és válasszuk a *Megnyitás* gombot. Fontos, hogy a sablonok jó része egymásra alapul (pl. a Hisec WS nem tartalmaz minden beállítást, amit a Secure WS) ezeket egymásra építve kell végrehajtani. Miután ez megtörtént, megjelenik egy ablak, melyben kiválaszthatjuk, hogy melyik sablont szeretnénk az adatbázisba felvenni, jelen esetben válasszuk a *Secure Ws*-t. Mivel később ebbe az adatbázisba más sablonok is importálhatók (ebben az esetben a beállítások kombinálódnak, illetve a metszetek felülíródnak), az *Adatbázis kitisztítása importálás előtt* funkció segítségével biztosíthatjuk, hogy csak ez a sablon érvényesüljön. Miután jóváhagytuk a sablon kijelölését, visszatérünk az MMC főablakába, és a *Biztonsági konfiguráció és analízis funkción* állva a jobb oldali ablakrészben megjelenik a használandó adatbázis neve (hisec.sdb).

Mint az ablakrész hátralevő részében lévő kis segítség is mondja, két lehetőségünk van. Az egyik a számítógép elemzése, az adatbázis alapján végrehajtódik az adott gép analizálása, az eltérések láthatóvá válnak. Ebben az esetben konfigurálás, átállítás nem történik. A másik a számítógép konfigurálása: az adott gépet átállítja az adatbázisnak megfelelően.



Érdemes a következő módszert választani. Először elemezzünk, nézzük át a változtatásokat, melyeket az adatbázis elvégezne, majd ha minden rendben, konfigurálhatunk.

Jótanácsok

Ez a kis segédprogram sok esetben rendkívül hasznos lehet:

Nagyobb cégeknél fordulhat elő, hogy különböző külső, vagy belső minőségellenőrzési szempontokból fontos lehet, hogy rendszeresen ellenőrizzék, hogy az informatikai rendszerük megfelel-e a szabványoknak. Ebben az esetben ez a feladat nagymértékben leegyszerűsíthető az eszközzel, hiszen csak a meg-

felelő sablonnal (amely származhat akár külső, minőségbiztosítási cégtől is) kell elemezni a gépeket, és azonnal láthatóvá válnak az esetleges eltérések.

Egy másik eset. Bármilyen intézménynél – beleértve az iskolákat is – az általános célú programokon kívül (Pl. Office) használnak különböző, többékevésbé egyéni alkalmazásokat is. Ahhoz, hogy ezeket védjük az esetleges törléstől, rongálástól, megfelelő jogosultságokat (NTFS) kell beállítanunk, tipikusan több fájlon és mappán. Az eszköz abban tud segíteni, hogy elég egyszer, egy adott gépen kikísérletezni a megfelelő beállításokat, majd ezeket kiexportálni egy sablonba, majd ezt a sablont a többi gépre is érvényesítve sok fáradságtól kímélhetjük meg magunkat.

A rendszerjavító csomagok (Service Packs)

Egy olyan operációs rendszernél is, mint a Windows 2000 elkerülhetetlenek előbukkanó, rejtett biztonsági és stabilitási problémák, melynek jó részét az újabb és újabb rendszereszközök és programok megjelenése idéz elő. Ezen problémák kiküszöbölésére jelennek meg az ún. Service Pack-ek, melyet a meglévő operációs rendszerre telepítve ezeket a „hibákat" megjavíthatjuk. Ezek a javítások szinte kivétel nélkül ingyenesek, és szabadon hozzáférhetők. Ahhoz, hogy rendszerünk jól működjön, elengedhetetlen alap a legújabb javítócsomagok telepítése. Ezen csomagok telepítése egyszerű, legtöbbször automatikus. A Windows 2000 újdonsága, hogy támogatja az ún. *Service Pack Slipstreaming* módszert, mely lehetővé teszi, hogy a rendszer bármi nemű változtatás esetén ne az eredeti fájlokat, hanem a javított fájlokat másolja fel. A módszer segítségével elkerülhető az a kellemetlenség, mely a régebbi NT verziók esetén fordult elő: ha valami megváltozott, az eredeti lemezről kerültek felmásolásra a rendszerfájlok, a megfelelő javítócsomagot minden egyes alkalommal újra kellett telepíteni.

A rendszerjavító csomagokat a következő útvonalról tölthetjük le: *http://www.microsoft.com/downloads.*

Hogyan növelhetjük hálózatunk biztonságát?

Ebben a fejezetben áttekintjük, milyen szempontokat érdemes egy hálózat biztonságánál figyelembe venni.

A munkaállomások

Ha lehetőségünk van, a kliensekre Windows 2000 Professional-t telepítsünk. Ha erre nincs lehetőségünk, akkor nézzük meg, hogy milyen operációs rendszer választásánál mire kell figyelnünk.

A Szerver

Egy jó, biztonságos hálózat alapja a megfelelő szerver gép:

A Server hardverének nem csak erősnek, hanem *stabilnak* is kell lennie, ne használjunk benne nem elég megbízható eszközöket, vagy olyanokat, melynek az eszközmeghajtó programjai (driver) nem megbízhatók, nem stabilak.

A „kék halál" (az a kék színű képernyő, mely a Windows 2000 esetleges megfagyásánál jelenik meg) védekezési mechanizmus, egy „biztosíték", általában a rendszer egy nagyobb sérüléstől védi így magát. A kék halál többnyire (kb. 70%-ban) akkor következik be, ha *egy adott eszköz* (pl. hálózati kártya), vagy annak meghajtó programja nem megfelelően működik, ezáltal veszélyeztetve a rendszer adatait. Ha a jelenség adott művelethez, eseményhez vagy eszközhöz köthető, akkor cseréljük ki az adott eszközt, vagy konfiguráljuk át, mert ebben a kiépítésben/beállításban veszélyezteti a rendszer egészét.

A Server telepítésénél általánosan javasolható, hogy csináljunk *külön partíciót* (vagy külön merevlemezt) a rendszernek, és másik(ak)at az adatoknak. A rendszerpartíciót érdemes NTFS fájlrendszerrel használni, így jelentősen csökken a Server sérülékenysége mind a vírusokkal, mind a lemezről, más operációs rendszerből történő indításos rongálásokkal szemben.

Mindig használjuk a *legújabb* rendelkezésünkre álló Service Pack-et.

Ha bármit változtatunk a Server kiépítésén (pl. új kártyát helyezünk be), használjuk ki a *Hardware profilok* kínálta lehetőséget, csináljunk magunknak visszalépési lehetőséget.

Lehetőleg tartsuk a Server-t és a más, létfontosságú hálózati eszközöket (pl. HUB, Router) *zárt helységben*, ezzel is csökkentve a rongálás, feltörés esélyét.

Windows 9x kliensek

Az itt felsorolt problémák szinte mind abból fakadnak, hogy ennél a termékcsaládnál nem elsődleges szempont volt a biztonságos hálózati működés. Mivel a Windows 9x nem támogatja a helyi felhasználói adatok védelmét (nem rendelhetünk hozzáférési jogosultságokat az állományokhoz), ezért a legnagyobb gond az, hogy holott a hálózaton keresztüli adatok hozzáférését tudjuk kontrolálni, de a helyi felhasználó működését nem tudjuk kellő módon korlátozni. Bár policy-vel megszabhatjuk, hogy a Windows 9x hogyan, miként működjön, ez elsősorban a munkakörnyezetre vonatkozik, és azt nem tudjuk vele megakadályozni, hogy egy felhasználó ne törölhesse le magát a rendszert, vagy az egyik programot a helyi gépről. A biztonságot az alábbi eszközökkel növelhetjük:

Policy-vel szabályozzuk, hogy ne lehessen a bejelentkezést megkerülni (pl. *ESC*, vagy *Mégse* gombbal), így legalább azt biztosíthatjuk, hogy csak az kapja meg a Windows felületet, akit hitelesített a Server. Ennek a módszernek is megvan a maga hátránya, ugyanis ilyenkor a hálózat nélküli működéssel a gépnek

gondjai lehetnek, adott felhasználók (akik még nem használták a gépet) nem fognak tudni belépni.

Állítsuk be úgy a gépeket, hogy *csak merevlemezről tudjanak elindulni*. Ezt általában a korszerűbb gépek SETUP-jában tehetjük meg. A beállítás módja benne van a gép (alaplap) leírásában. Ezt azért célszerű megtenni, mert így elkerülhetjük, hogy a gépet és az adatokat a Windows 9x megkerülésével, lemezről indítva érjék el.

A *felhasználók adatait* (profil, home könyvtár) lehetőleg tároljuk a Server-en lévő megosztásokon, ugyanis a Windows 9x elején lévő belépés csak a felhasználói környezet (profil) kiválasztására alkalmas, ha valaki belépett, akkor a helyi gépen lévő minden adatot teljes joggal elérhet, módosíthat, törölhet.

Ha hálózati *home könyvtárakat* akarunk használni, ne felejtsük el, hogy a könyvtár csatlakoztatása belépéskor nem történik meg automatikusan, hanem szükség van *Login Scriptre*, mely a csatlakoztatást elvégzi. Ezt a *NET USE H: /HOME* parancs kiadásával lehetséges.

Windows 2000 (Windows NT) munkaállomások

A hálózat szempontjából sokkal ideálisabbak ezek a munkaállomások, hiszen ezekbe az operációs rendszerekbe már beépítették a hálózati működést, illetve a helyi adatok védelmének lehetőségét (persze ehhez NTFS-t kell helyileg is használnunk).

Az egyik legfontosabb különbség az előzőkhöz képest, hogy itt lehetőségünk van magára a munkaállomás védelmére is. Maga a Windows NT is már védi a rendszerállományait véletlenszerű törlés ellen. Ezen túlmenően lehetőségünk van alkalmazásaink, programjaink, sőt egész helyi rendszerünk védelmére is, igaz, ez a kikísérletezés fázisában, igen munka- és időigényes feladat, és középszintű hozzáértést feltételez. A dolog a következő módon működik.

Installáljunk fel egy gépet, tegyük rá a kívánt alkalmazásokat, állítsuk be azokat. Ha ezeket az alkalmazásokat meg akarjuk védeni, akkor annak egy módja van, fájlrendszer szinten védeni kell a fájlokat módosítás és törlés ellen. Például a *C:* meghajtó főkönyvtárából végigeresztünk egy NTFS jogosultságosztást a következő beállításokkal:

Mindenki – olvasás
Administrators csoport – Teljes elérés
Rendszer (SYSTEM) – Teljes elérés

Mivel vannak olyan helyek, ahova a rendszer a felhasználó nevében kénytelen, hogy tudjon írni, ilyen például a *TEMP* könyvtár. Ezeknek a könyvtáraknak *Mindenki – teljes elérés* jogot kell adni. Hogy hogyan találhatjuk meg ezeket a könyvtárakat, állományokat? Kísérletezéssel! Elindulunk a legszigorúbb jogokból, és kipróbáljuk, hogy minden működik-e. Ha nem, nézzük meg, mi a baj (ebben segít a naplózás), és az érintett állománynak (vagy könyvtárnak) több jogot adunk, stb…

Felhasználók

Pár jótanács a felhasználók kezeléséhez:

A *Rendszergazda* felhasználót nevezzük át valami olyan felhasználói névre, mely nem tűnik ki a felhasználók listájából.

Praktikus a *Vendég*, vagy valamely nulla jogú felhasználót átnevezni *Rendszergazdára*, hogy ha próbálkoznak, és feltörik a jelszót, akkor kellemetlen meglepetés érje őket.

Sohase használjuk a tényleges *Rendszergazda* felhasználót, az maradjon meg biztonsági tartaléknak, és állítsuk be, hogy ne járhasson le a jelszava, nehogy kizárjuk magunkat. Készítsünk magunknak egy *rendszergazda jogú* felhasználót (pl. GipszJ), adjuk hozzá a *Vállalati Rendszergazdák (Enterprise Admins)* csoportba, és ezt a felhasználót kizárólag csak adminisztratív feladatok ellátására használjuk! A napi teendők elvégzésére mi is csak egy általános jogú felhasználót használjunk, csökkentve ezzel is a felesleges kockázatot.

Ha mindig rendszergazdai jogokkal vagyunk a hálózatban, úgy vegyük figyelembe a következőket:

Növekszik a vírusfertőzések illetve a trójai programok által véghezvitt pusztítások esélye, mivel minden program (beleértve a vírust és a trójait is) ilyenkor rendszergazdai kontextusban fut, azaz mindent elérhet, amit maga a felhasználó interaktívan.

Egy esetleges véletlen kilépés, vagy zárolás nélküli „gépelhagyás" esetén más, a géphez hozzáférő felhasználók szintén rendszergazdai jogokkal bírnak.

Mivel a rendszergazda a napi munkájához is „teljes jogú" környezetben fut, esetlegesen nem kap első kézből visszajelzést azokról a problémákról, melyek egy „halandó" felhasználó számára merülnek fel.

Mindig nevesítsük felhasználóinkat, sokkal egyszerűbb a hálózat kézbentartása, ha nem *általános tanuló* felhasználói néven lép be mindenki, hanem beazonosítható felhasználói néven.

Ha adminisztratív feladatokat adunk ki kezünkből (pl. felhasználói adatbázis karbantartása), akkor az illetőnek *csak annyi többletjogot* adjunk, ami a feladata elvégzéséhez feltétlen szükséges. Például a felhasználói adatbázis kezeléséhez az adott segéd-rendszergazdának az AD csak megfelelő ágát delegáljuk szerkesztésre, a többit ne adjuk ki kezünkből.

Követeljük a jelszó *minimális hosszát* (min. 6 karakter), a maximális élettartamát (30 nap), minimális élettartamát (3 nap), és egyedi jelszó igénylését (5).

Használjuk a *kizárást* a jelszó próbálgatásos betörések ellen.

Hozzáférési jogosultságok

Az *adminisztráció leegyszerűsítése* céljából csoportosítsuk adatainkat három csoportba: alkalmazások, adatok, home könyvtárak. Így a következő előnyökhöz juthatunk.

A jogosultságokat általánosságban elég könyvtár szinten megadni, fájl szinten csak ritkán kell módosítani.

A biztonsági mentés jóval egyszerűbb. A prioritás a következő: home könyvtárak, adatok, alkalmazások.

Az összes home könyvtár egy helyen van.

Használjunk *NTFS jogosultságokat* a mappák és fájlok elérésének korlátozásához. Tartsuk magunkat a minimálisan elégséges jogok osztása szemléletet, ezzel is csökkenthetjük a veszélyét, hogy a felhasználó véletlenül, vagy szánt szándékkal fontos fájlokat módosítson, vagy töröljön.

Lehetőleg *csoportokat használjunk* a hozzáférési jogosultságok kiosztásánál, kerüljük az egyéni felhasználók használatát, hacsak nem feltétlen szükséges.

Az alkalmazás- és a munkamappáknál figyeljünk arra, hogy távolítsuk el az alapértelmezett *Mindenki – Teljes elérés* jogot, és rendeljünk hozzá helyette a Tartomány-felhasználóknak és Rendszergazdáknak *Olvasás és Végrehajtás* jogot. Ezzel megelőzhetjük az esetleges fájl törléseket és módosításokat, vagy az esetleges vírusfertőzést. Azoknak a felhasználóknak és rendszergazdáknak, melyek ezen alkalmazások üzemeltetéséért, frissítéséért felelősek, a munkájuk elvégzésének idejére megkaphatják a teljes elérés jogot, majd ha végeztek, érdemes ezt megszűntetni.

Nyilvános, közös mappák esetén rendeljünk *módosítási*, *olvasási* és *végrehajtási* jogot a felhasználóknak, és *teljes elérést* a létrehozó tulajdonosnak. Ez lehetővé teszi, hogy mindenki csak a saját maga által létrehozott állományokat módosíthassa és törölhesse, viszont olvashassa a többiek által létrehozott dokumentumokat.

A *tiltó jogosultságokat* csak akkor használjuk, ha kifejezetten „kizárás” a szándékunk, más esetben jobb, ha egy jogot nem rendelek hozzá, mintha tiltom.

Az NTFS szintű *jogdefiniálásnál* tartsuk szem előtt a következőket:

Ha egy felhasználó mind egyéni, mind csoportszinten kap jogokat, mindig ezek összessége lesz az effektív joga. Példa: ha egy felhasználó egyéni szinten olvasási, csoport szinten módosítási joggal rendelkezik egy fájlra, akkor az ő effektív joga olvasás + módosítás lesz.

Az NTFS fájl jogosultságok erősebbek az NTFS mappa jogosultságoknál, még akkor is, ha a mappára nincs elérési joga, a közvetlen címzéssel a fájl elérhető lesz.

A tiltó bejegyzések mindig erősebbek az engedélyezőknél, akár csoport, akár egyéni szinten kapjuk. Példa: Egy állományra *Mindenki – Teljes jog* van definiálva, de az adott felhasználónak van egy törlést tiltó bejegyzése is. Ő olvashatja és módosíthatja is a fájlt, de törölni nem tudja.

Alapból a jogosultságok mindig öröklődnek a szülőmappákról az almappákra, de ez az öröklődés blokkolható.

Egy új állomány mindig a szülőmappája jogosultságát örökli.

Lehetőség van az örökölt jogosultságok módosítására újabb jogosultság bejegyzések létrehozásával.

Egy adott objektum hozzáférési jogosultságait az tudja megváltoztatni, aki rendelkezik az objektumra a *Hozzáférési jogok módosítása* joggal. Ez természetesen része a *Teljes elérésnek*.

Minden objektum rendelkezik tulajdonossal, mely az a felhasználó, aki létrehozta. A tulajdonos mindig képes a jogosultságok megváltoztatására, még akkor is, ha nem szerepel a jogosultságlistában. A tulajdonjog átvehető – viszont nem átruházható – a *Saját tulajdonba vétel* jog segítségével.

Ha egy objektumot egy olyan felhasználó veszi tulajdonba, aki tagja a Rendszergazdák csoportnak, az objektum tulajdonosa nem a felhasználó, hanem a csoport lesz.

Ha NTFS jogosultságokkal ellátott objektumokat másolunk, vagy mozgatunk, a jogosultságok megváltozhatnak, a következők szerint: Az objektum mindig örökli a célmappa jogosultságait (másolás partíción belül és kívül, illetve áthelyezés partíción kívül), kivéve ha az objektumot partíción belül mozgatjuk.

Megosztások

A megosztási jogosultságok mindig mappára érvényesülnek, nem különálló fájlokra. Mivel csak egész mappákra definiálhatunk jogot, ez a fajta jogosultságosztás nem olyan kifinomult, és jól definiálható, mind az fájlrendszer (NTFS) szintű jogosultságok, ahol fájl szintre is lemehetünk.

A megosztási jogosultságok nem érvényesülnek azon felhasználókra, akik helyileg az adott gépen ülnek, ahol a megosztott erőforrások vannak, és közvetlenül, fájlszinten érik el azokat. Ezek a jogosultságok csak a hálózati elérésen keresztül érvényesülnek.

FAT-os partíciókon a megosztási jogosultság az egyetlen módszer az elérés korlátozására, mivel itt nincsen fájlrendszer szintű jogosultságosztás.

Ha egy adott mappára mind megosztás, mind NTFS szinten definiálunk jogokat, mindig a megszorítóbb kerül érvényre (hálózaton keresztül – hiszen ha lokálisan férünk hozzá, a megosztási jogosultságok nem befolyásolják a működést, hiszen nem használjuk a megosztást).

Az alapértelmezett megosztási jogosultság (kivéve az adminisztrátori megosztásokat) *Mindenki – Teljes elérés*. Ha NTFS szintű jogosultságokat osztunk az adott mappára, akkor ezt nyugodtan hagyhatjuk így, hacsak nem valami speciális beállítás elérése a cél.

Egy adott mappát többszörösen is megoszthatunk, különböző megosztási nevekkel és jogosultságokkal.

Az adminisztratív megosztások (*C$,Admin$*, stb.) alapértelmezett megosztási jogosultsága: *Rendszergazdák – Teljes elérés*.

Hibakeresés

A hiba leírása	Lehetséges okok, megoldások
Egy felhasználó nem tud hozzáférni egy adott fájlhoz vagy mappához	Ellenőrizzük le, hogy milyen jogosultságok vannak definiálva az objektumra, mind felhasználó, mind azon csoportok szintjén, melynek a felhasználó tagja. Akár a felhasználónak, akár bármely csoportjának elérést tiltó joga van, a felhasználó nem férhet az objektumhoz. Ha az objektumot másoltuk egy NTFS partíción belül, vagy másoltuk illetve átmozgattuk egy másik NTFS partícióra, az objektum eredeti jogosultságai esetlegesen megváltoztak, örökölvén az új szülőmappa (célmappa) jogosultságait. Ha a mappára mind NTFS, mind megosztási jogosultságok is definiálva vannak, de akkor a szigorúbb érvényesül! Ezért, az egyszerűség kedvéért (hacsak nem szükség van rá) állítsuk a megosztási jogosultságot Mindenki – Teljes elérésre, és csak NTFS szinten definiáljunk jogokat.
Egy felhasználói fiókot hozzáadtunk egy csoporthoz, melynek joga van az erőforrás elérésére, de a felhasználó még mindig nem éri el azt.	Egy jogosultságkártya (Access Token) keletkezik minden alkalommal, mikor egy felhasználó bejelentkezik és hitelesítődik egy NT vagy 2000 által. Ez a kártya tartalmaz információkat a felhasználó csoporttagságával kapcsolatosan. Ahhoz, hogy ez a kártya frissítődjön és az esetleges csoporttagság változások érvényre jussanak, a felhasználónak ki kell lépni, majd újból belépni.
Egy felhasználó letörölt egy fájlt annak ellenére, hogy nincs törlési joga.	Definiáljuk a jogosultságokat mappa szinten, ne fájl szinten, tehát csoportosítsuk a fájlokat mappákba úgy, hogy ez kivitelezhető legyen. Az ok egyébként a mappán élvezett Teljes jogból adódik, ez ugyanis lehetővé teszi, hogy egy akár „elérhetetlen” fájlt is törölni tudjunk. Ha a Teljes jogkör kiosztása elkerülhetetlen, a Teljes jog helyett rendeljük hozzá egyenként az összetevőit: Módosítás, Olvasás és Végrehajtás, Mappák tartalmának olvasása, Olvasás, írás. Ezzel minden szükséges jogot megadtunk a teljes működéshez, kivéve a törlést.