Microsoft Business Solutions

# Navision Security Hardening Guide

Készült: 2004. október

Microsoft

# Tartalom

# Bevezetés

A Microsoft® Windows® korszerű, szabványokon alapuló hálózati biztonságot szavatol. A szó legtágabb értelmében véve a biztonsághoz hozzátartozik a tervezés és a kompromisszumok figyelembevétele is. A számítógép például elhelyezhető lezárt szobában úgy, hogy csak egy rendszergazda férjen hozzá. Ez a számítógép ugyan biztonságos, de nem túl hasznos, mert nem csatlakozik más számítógépekhez. A hálózatot anélkül kell minél biztonságosabbá tenni, hogy ez a hasznossága rovására menne.

A legtöbb szervezet a külső támadások ellen tűzfallal védekezik, de legtöbbjük nem foglalkozik a tűzfalon esetlegesen áttörő kalózok elleni védelemmel. Az ügyfélkörnyezet biztonsági intézkedései akkor működnek megbízhatóan, ha a felhasználóknak nem kell túl sok műveletet vagy lépést végrehajtaniuk a biztonság szavatolása érdekében. A biztonsági házirendek bevezetését úgy kell megvalósítani, hogy a lehető legkevesebb tennivalóval járjon a felhasználók számára, különben hajlamosak figyelmen kívül hagyni a teendőket.

Mivel a Navision telepítési mérete nagy tartományban mozoghat, célszerű pontosan meghatározni az egyes ügyfelek szükségleteit, és összevetni a felmerülő költségeket a biztonsági intézkedések hatékonyságával. Mivel ügyfelei megbíznak Önben, döntsön megfontoltan, és olyan irányelvet javasoljon nekik, amely anélkül tesz eleget biztonsági szükségleteiknek, hogy a betarthatóságot veszélyeztető terheket róna rájuk.

# A Navision biztonságával kapcsolatos gyakorlati tanácsok

A következő általános szabályokkal javíthatja a Navision környezet biztonságát:

- Ha a Navision Database Server kiszolgálót szolgáltatásként szeretné futtatni, vagy a kiszolgáló indításakor az *installasservice* parancsot használja, akkor győződjön meg róla, hogy a szolgáltatás az NT Authority\Hálózatszolgáltatás fiókon fut. Az NT Authority\Hálózatszolgáltatás fiók csak Windows™ XP és Windows Server™ 2003 rendszereken létezik. Windows 2000 Server rendszeren hozzon létre a szolgáltatás számára egy fiókot a lehető legkevesebb jogosultsággal, mert enélkül a szolgáltatás Helyi rendszer fiókhoz lesz rendelve. A fiók legfeljebb azokkal a jogosultságokkal rendelkezzen, amivel a szokásos Felhasználók fiók, vagy legyen olyan tartományi fiók, amely nem rendszergazda sem a tartományban, sem a számítógépen.

  Ne felejtsen az NT Authority\Hálózatszolgáltatás fióknak vagy a szolgáltatást futtató felhasználói fióknak írási és olvasási jogot adni az adatbázisfájl(ok)ra, mert enélkül a felhasználók nem csatlakozhatnak az adatbázishoz.

  Az NT Authority\Hálózatszolgáltatás fióknak Windows XP rendszeren a következőképpen adhat írási és olvasási jogot az adatbázisfájlra:

  1. A Windows Intézőben nyissa meg az adatbázisfájlt tartalmazó mappát.
  2. Jelölje ki az adatbázisfájlt, kattintson rá a jobb gombbal, majd kattintson a Tulajdonságok parancsra.
  3. A ***Tulajdonságok*** panel ***Biztonság*** lapján, a **Csoport- és felhasználónevek** mezőnél kattintson a Hozzáadás gombra.
  4. A ***Felhasználók, számítógépek vagy csoportok kijelölése*** panelen írja be a *Hálózatszolgáltatás* szót, és kattintson az OK gombra.
  5. A HÁLÓZATSZOLGÁLTATÁS bekerült a ***Tulajdonságok*** panel **Csoport- és felhasználónevek** mezőjébe.
  6. Jelölje ki a HÁLÓZATSZOLGÁLTATÁS elemet, és az **Engedélyek** mezőben adjon neki *Olvasás* és *Írás* engedélyt.

- A Navision Application Server szolgáltatás alapértelmezés szerint az NT Authority\Hálózatszolgáltatás fiókon fut, így helyileg elérheti a Navision Database Server kiszolgálót. Hálózaton azonban meg kell bizonyosodni róla, hogy a Navision Application Server szolgáltatás a Navision Database Server által felismert Windows tartományfiókon fut, különben nem éri el az adatbázis-kiszolgálót. Ez a fiók ne legyen rendszergazda sem a tartományban, sem a helyi számítógépeken.

- Az SQL Server Option for Navision használata esetén a Microsoft SQL Server™ fut szolgáltatásként. Az SQL Server Option for Navision használatához szükséges, hogy az SQL Server hitelesítési célból Windows felhasználói csoportokat kereshessen az Active Directoryban. Ezért győződjön meg róla, hogy az SQL Server szolgáltatás az NT Authority\Hálózatszolgáltatás fiókon fut.

  Ennek ellenőrzéséhez tegye a következőket:

  1. Az SQL Server programot futtató számítógépen keresse meg az MSSQLSERVER szolgáltatást, kattintson rá a jobb gombbal, majd kattintson a Tulajdonságok parancsra.
  2. A ***Tulajdonságok*** ablakban kattintson a ***Bejelentkezés*** fülre.
  3. A ***Bejelentkezés*** lap Bejelentkezés mint beállításánál válassza az Ez a fiók lehetőséget, és írja be az *NT Authority\Hálózatszolgáltatás* nevet, majd kattintson az OK gombra.

  Az SQL Server biztonságával kapcsolatban további tájékoztatást az alábbi webhelyeken talál:

  http://www.microsoft.com/security/guidance/prodtech/SQLServer.mspx

  és

  http://www.microsoft.com/technet/security/prodtech/dbsql/default.mspx

- Ha Navision E-business terméket, például a Commerce Gateway programot futtatja, győződjön meg róla, hogy a Commerce Gateway Request Server megfelelően, a szolgáltatásokra vonatkozó alapértelmezett fiókbeállításokkal lett telepítve. Az alapértelmezett fiókbeállítás neve *CGRSUser*. Ez a beállítás csak a feltétlenül szükséges egyéb szolgáltatásokhoz biztosít hozzáférést a Commerce Gateway Server kiszolgálónak, például az *MSSQLSERVER* szolgáltatáshoz és a *BizTalk Service BizTalk Group : BizTalkServerApplication* alkalmazáshoz, és nem tartalmaz semmilyen globális fiókbeállítást, mint például a *Local System* fiók.
- Mindig erős jelszót használjon. Az erős jelszavakkal kapcsolatban az Erős jelszavak című szakaszban olvashat bővebben.
- Használjon Windows bejelentkezést. A Navision kétféle bejelentkezéssel használható: adatbázis-bejelentkezéssel és Windows bejelentkezéssel. A Windows bejelentkezés ajánlott, mivel ez a módszer a Windows hitelesítését használja, és megfelelő jelszóházirend betartatására nyújt lehetőséget.
- A jelszavakat nem szabad újra felhasználni Gyakorta megesik, hogy a rendszer- és tartományjelszavakat újra felhasználják. Előfordulhat például, hogy egy két tartományt felügyelő rendszergazda mindkét tartományhoz ugyanazt a rendszergazdai jelszót adja meg, és még a tartományi számítógépek helyi rendszergazdai jelszavát is mindenütt ugyanerre állítja be. Ebben az esetben egyetlen fiók vagy számítógép biztonságának sérülése a teljes tartomány biztonságát veszélyezteti.
- A Navision telepítése és az adatbázisok létrehozása vagy frissítése után hozzon létre egy Windows felhasználót, és rendelje a Navision SUPER szerepköréhez. Ez a SUPER felhasználó kezeli az adatbázis-felügyeletet, a biztonságot stb. Adjon meg erős jelszót a felhasználóhoz. Ezt a jelszót tartsa titokban. Ugyanolyan védelem alá kell esnie, mint az SQL Server SA-jelszavának. A SUPER szerepkör kezeli az összes adatbázis-hozzáférést, így a legmagasabb szintu védelem illeti meg. A SUPER felhasználó jelszavát csak a rendszergazdáknak árulja el.
- A Navision adatbázishoz hozzáférő többi felhasználó a lehető legkevesebb jogosultságot kapja meg. Ennek megfelelően olyan Navision szerepkört rendeljen hozzájuk, amely csak az általuk elvégzendő vállalati feladatok teljesítéséhez feltétlenül szükséges funkciókhoz való hozzáférést biztosítja.
- Győződjön meg róla, hogy csak azok a felhasználók tudnak FOB fájlokat importálni, objektumokat áttervezni, illetve biztonsági másolatokat készíteni és visszaállítani, akiknek a vállalati szerepköre ezt indokolja.
- Készítsen rendszeresen biztonsági másolatokat a Navision adatbázisról, és tesztelje ezek visszaállíthatóságát.
- A biztonsági másolatokat tárolja biztonságos helyen, tűztől, füsttől, portól, hőtől, villámcsapástól és egyéb környezeti katasztrófáktól (pl. földrengéstől) védve.
- Bár a Navision a Windows több verzióján is használható, ajánlott a legújabb biztonsági szolgáltatásokkal ellátott legfrissebb operációs rendszerek használata. Jelenleg ezek a rendszerek a Windows XP Service Pack 2 és a Windows Server 2003.
- A Windows 2000, Windows XP és Windows Server 2003 rendszerek Windows Update szolgáltatásával rendszeresen telepítse az új biztonsági frissítéseket. A Windows automatikus frissítési szolgáltatásával felhasználói közreműködés nélkül telepítheti az összes ügyfélgépre a biztonsági javításokat, szervizcsomagokat és frissítéseket.
- A Navision ügyfelek és a Navision Database Server közötti kommunikációhoz használjon biztonságos TCPS protokollt. A TCPS a TCP/IP biztonságos változata, amely Security Support Provider Interface (SSPI) felületet, titkosítást és Kerberos hitelesítést használ. A TCPS Navision Database Server alapértelmezett protokollja.
- Az ügyfélnek rendelkeznie kell vészhelyreállítási tervvel, amely katasztrófahelyzetben biztosítja a szolgáltatások gyors helyreállítását. A helyreállítási tervnek többek közt a következőket ajánlott tartalmaznia:
    - Új vagy ideiglenes berendezések beszerzése
    - Biztonsági mentések visszaállítása az új rendszerre
    - A helyreállítási terv működőképességének tesztelése

# Fizikai biztonság

A fizikai biztonság létfontosságú, mert szoftveresen nem váltható ki. Ha például ellopnak és feltörnek egy merevlemezt, akkor a rajta lévő adatokat is ellopják. Az ügyfél biztonsági házirendjének kialakításakor a következő fizikai biztonsági szempontokat kell figyelembe venni:

- A számítástechnikai részleggel rendelkező nagy szervezeteknél a kiszolgálószobát és a szoftvertároló helyiségeket zárni kell.
- Az intézkedés hatálya alá kell essenek a következők:
  - a Microsoft SQL Server 2000 kiszolgáló
  - a Navision programfájljait tartalmazó fájlkiszolgáló.
- A jogosulatlan felhasználókat távol kell tartani a számítógépektől.
- Az adatok fontosságától függetlenül szereljen fel riasztót.
- A létfontosságú adatok másolatait a szervezet telephelyén kívül, tűzálló tárolókban kell tárolni.

# A dolgozók

A felügyeleti jogokat minden program és szolgáltatás esetében célszerű korlátozni. Alapértelmezés szerint az ügyfél csak olvasási jogot adjon dolgozóinak a rendszerfunkciókra, ha munkájuk elvégzéséhez nincs szükségük ennél tágabb hozzáférési körre. A Microsoft a legkisebb jogosultság elvét ajánlja: a felhasználók csak a mindenképpen szükséges adatokhoz és funkciókhoz kapjanak hozzáférési jogosultságot.
Az elégedetlen vagy a cégtől távozott dolgozók biztonsági kockázatot jelentenek. Az ügyféllel történő egyeztetéskor a dolgozókkal kapcsolatban a következő irányelvet javasolja:

- Az alkalmazásba vétel előtt informálódni kell a dolgozókról.
- Számítani kell az elégedetlen vagy a cégtől távozott dolgozók „bosszújára”.
- Ha a dolgozó távozik a cégtől, az összes vonatkozó Windows fiókot és jelszót le kell tiltani. A felhasználókat a különféle kimutatások készítése miatt nem célszerű törölni. A fiókokat nem szabad újra felhasználni.
- A felhasználókat éberségre és a gyanús tevékenységek jelentésére kell ösztönözni.
- Nem szabad automatikusan megadni semmilyen jogosultságot. Biztosítani kell, hogy a felhasználók ne férjenek hozzá azokhoz a számítógépekhez, szobákhoz vagy fájlcsoportokhoz, amelyekre nincs szükségük.
- A rendszergazdákat fel kell készíteni a dolgozókkal kapcsolatos biztonsági problémák felismerésére és kezelésére.
- A dolgozóknak meg kell magyarázni a hálózati biztonság fenntartásában játszott szerepüket.
- A vállalati biztonsági irányelveit minden dolgozónak ki kell osztani.
- Nem szabad engedélyezni, hogy a dolgozók a munkáltató által jóvá nem hagyott programokat telepítsenek.

## A rendszergazda

Az ügyfelek rendszergazdái számára ajánlott nyomon követni a Microsoft legújabb biztonsági javításait. A támadók gyakori módszere, hogy kisebb biztonsági rések együttes kihasználásával hajtanak végre nagyobb betöréseket. A rendszergazdának először is gondoskodnia kell az egyes számítógépek biztonságáról, majd telepíteni kell a biztonsági frissítéseket és a vírusellenőrző programot. Az útmutató számos, értékes információkra vagy gyakorlati tanácsokra mutató hivatkozást tartalmaz.

A hálózati biztonság szempontjából az összetettség is kritikus szempont. Minél bonyolultabb a hálózat, annál nehezebb biztonságban tartani, illetve a sikeres betörési kísérlet után helyreállítani. A rendszergazda minél egyszerubb hálózati topológia fenntartására és annak dokumentálására kell törekedjen.

A biztonság kérdése elsősorban a kockázatkezelésen alapul. Mivel a technika önmagában nem biztosít megoldást mindenre, tudatos intézkedésekkel kell kombinálni. Sosem lesz ugyanis olyan termék, amely automatikusan szavatolná a teljes hálózati biztonságot. A biztonság a technika és az irányelvek közös használatának gyümölcse. A hálózat biztonsági szintjét végső soron a technika használatának mikéntje szabja meg. A Microsoft a biztonságnak központi jelentőséget tulajdonító termékeket készít, de az egyes szervezetek számára megfelelő irányelveket csak a rendszergazda tudja meghatározni az Ön segítségével. A biztonságot már a hálózat kialakításának első szakaszaiban is figyelembe kell venni. Gondolja át, mit szeretne megvédeni az ügyfél, és mire hajlandó ennek érdekében.

Végül dolgozzon ki vészforgatókönyveket még a vészhelyzet beállta előtt. Az alapos tervezés és a megbízható technológia együtt szavatolja ügyfele biztonságát.

A biztonsággal kapcsolatban további általános felvilágosítást találhat a „The Ten Immutable Laws of Security Administration” (A biztonsági felügyelet tíz sziklaszilárd szabálya) címu dokumentumban a következő webhelyen:
http://www.microsoft.com/technet/archive/community/columns/security/essays/10salaws.mspx

A biztonság kezelésével kapcsolatos cikkek:
http://www.microsoft.com/technet/community/columns/secmgmt/smarch.mspx

## A kiszolgáló operációs rendszerének biztonsága

Bár sok kisebb ügyfél nem használ kiszolgálóhoz írt operációs rendszert, a nagyobb vállalatok összetettebb hálózati környezet miatt mégis fontos megismerkedni az ezekkel kapcsolatos gyakorlati tanácsokkal is. Az itt leírt irányelvek és tanácsok nagy része ügyfélrendszerekre is egyszerűen alkalmazható.

A jelen szakaszban leírtak egyaránt vonatkoznak a Microsoft Windows 2000 Server és Microsoft Windows Server 2003 rendszerekre, bár az információk forrása jórészt a Windows Server 2003 súgója. A Windows Server 2003 robusztus biztonsági szolgáltatásokkal rendelkezik. A Windows Server 2003 súgója átfogó ismertetést nyújt a biztonsági funkciókról és eljárásokról.

A Windows 2000 Server rendszerrel kapcsolatban a Windows 2000 Server Security Center webhelyen kaphat további tájékoztatást:
http://www.microsoft.com/technet/security/prodtech/win2000/default.mspx

Segítséget nyújthat még a Windows 2000 Security Hardening Guide című biztonsági útmutató:
http://www.microsoft.com/technet/security/prodtech/win2000/win2khg/default.mspx

A Windows Server 2003 rendszerrel kapcsolatban a Windows Server 2003 Security Guide útmutatóból kaphat további tájékoztatást:
http://www.microsoft.com/technet/security/prodtech/win2003/w2003hg/sgch00.mspx

A Windows kiszolgáló-biztonsági modell alapvető elemei a hitelesítés, a hozzáférés-vezérlés és az egységes bejelentkezés:

- A hitelesítés során a rendszer a bejelentkezési hitelesítő adatok alapján a rendszer ellenőrzi a felhasználó kilétét. A felhasználó nevét és jelszavát a rendszer egy hitelesített listán keresi meg. Egyezés esetén a hitelesítés révén a felhasználó az engedélylistán megadott mértékben hozzáférést nyer a rendszerhez.
- A hozzáférés-vezérlés a felhasználó azonossága és előre megadott csoportokban való tagsága alapján szabályozza az információkhoz vagy erőforrásokhoz való hozzáférést. A rendszergazdák általában így szabályozzák, hogy a felhasználók milyen hozzáféréssel rendelkezzenek a hálózati erőforrásokhoz, például kiszolgálókhoz, könyvtárakhoz vagy fájlokhoz. A hozzáférés-vezérlés általában az egyes objektumokra vonatkozó, a felhasználóknak és csoportoknak megadott engedélyek által valósul meg.
- Az egységes bejelentkezés révén a felhasználó, ha egyszer, egyetlen jelszóval belépett a Windows tartományba, az abban lévő összes gépre hitelesítheti magát. Így a rendszergazdák a Windows hálózat szintjén valósíthatják meg a jelszóhitelesítést, és felhasználóiknak egyszerű hozzáférést biztosíthatnak.

A következő szakaszokban a három alappillér részletesebb ismertetése olvasható.

## Hitelesítés

A hitelesítés a rendszerbiztonság alapvető szempontja. Ennek révén egyértelműsítheti azonosságát a tartományba bejelentkezni, vagy annak erőforrásait elérni szándékozó felhasználó. A legtöbb hitelesítési rendszer leggyengébb láncszeme a felhasználó jelszava.

A jelszó a tartományi és helyi számítógépek jogosulatlan elérése elleni első védelmi vonal. A jelszavakkal kapcsolatos legfontosabb gyakorlati tanácsok:

- Mindig erős jelszót használjon.
- Ha a jelszót le kell írni, akkor a papírt tárolja biztonságos helyen, és ha már nincs rá szükség, semmisítse meg.
- Soha ne mondja el senkinek a jelszavát.
- Minden felhasználói fiókhoz használjon más jelszót.
- A jelszót rendszeres időközönként változtassa meg.
- Ügyeljen arra, hogy a számítógépen hová menti a jelszavakat.

## Erős jelszavak

A jelszavak szervezeti biztonságban játszott szerepét gyakran alábecsülik. Mint korábban említettük, a jelszavak képezik a hálózat jogosulatlan elérése elleni első védelmi vonalat. Ennek megfelelően gondoskodjon róla, hogy ügyfelei megkövetelik dolgozóiktól az erős jelszavak használatát.

A jelszófeltörő eszközök azonban fejlődnek, a feltöréshez használt számítógépek pedig egyre nagyobb teljesítménnyel bírnak. Elegendő idő alatt az automatikus jelszófeltörő eszközök bármilyen jelszót fel tudnak törni. Az erős jelszavakat azonban sokkal nehezebb feltörni, mint a gyengéket.

A megjegyezhető, mégis erős jelszavak megalkotásával kapcsolatban a következő címeken talál további tájékoztatást:

http://www.microsoft.com/athome/security/privacy/password.mspx

és

http://www.microsoft.com/ntworkstation/technicalresources/PWDguidelines.asp

## A jelszóházirend meghatározása

Ügyeljen rá, hogy olyan jelszóházirendet állítson össze, amely minden felhasználói fiók esetén megköveteli az erős jelszavak használatát. A legtöbb rendszer esetén elegendő követni a Windows Server 2003 biztonsági útmutatójában foglaltakat:

- Az **Előző jelszavak megőrzése** házirend-beállításnál adja meg a jelszavak tárolását. Így a felhasználók nem állíthatják ismét be a lejárt jelszót.

  Ajánlott érték: 24

- A **Jelszó maximális élettartama** házirend-beállításnál adjon meg az ügyfél környezetének megfelelő értéket.

  Ajánlott érték: 42 (alapértelmezett) – 90.

- A **Jelszó minimális élettartama** házirend-beállításnál adhatja meg, hogy a jelszót hány napig nem lehet módosítani. Ez a beállítás az **Előző jelszavak megőrzése** beállítással együtt használatos. Ha meg van adva a minimális élettartam, a felhasználók nem módosíthatják gyors egymásutánban többször a jelszavukat, így nem tudják megkerülni az **Előző jelszavak megőrzése** beállítást, hogy újra régi jelszavukat használják. Ehelyett a megadott számú napig várniuk kell a jelszómódosítással.

  Ajánlott érték: 2.

- A **Legrövidebb jelszó** házirend-beállításnál adhatja meg, hogy a jelszavaknak legalább hány karakterből kell állnia. A hosszú, hét vagy több karakteres jelszavak általában erősebbek, mint a rövidek. A beállítás révén a felhasználók nem adhatnak meg üres jelszót, illetve alkalmazkodniuk kell a megadott korlátokhoz.

  Ajánlott érték: 8.

- Engedélyezze **A jelszónak meg kell felelnie a bonyolultsági feltételeknek** házirend-beállítást. Ez a beállítás ellenőrzi, hogy az új jelszavak megfelelnek-e az erős jelszavak alapvető követelményeinek. A beállítás azt vizsgálja meg, hogy a jelszóban szerepel-e összesen legalább három jel a négy kategóriából (kisbetu, nagybetu, szám, nem

alfanumerikus jel), illetve hogy a jelszó nem tartalmazza a felhasználónév, vagy a felhasználó család- vagy vezetékneve valamely részét.

**Megjegyzés**
Az ezen követelményeknek eleget tevő jelszavak sem feltétlenül nagyon erősek. A „Jelszó1” jelszó például megfelel a feltételeknek.

Ajánlott érték: Igen

- A követelmények teljes listája a Windows Server súgójának „A jelszónak meg kell felelnie a bonyolultsági feltételeknek” című témakörében található.
- A jelszavak tárolása visszafejthető titkosítással – A visszafejthető titkosítás olyan rendszerekben használatos, ahol egyes alkalmazásoknak a jelszavak egyszerű szöveges formájához kell hozzáférniük. A legtöbb esetben erre nincs szükség.

  Ajánlott érték: Nem.

További tájékoztatást a Windows Server 2003 Security Guide biztonsági útmutatóban találhat:

http://www.microsoft.com/technet/security/prodtech/Win2003/W2003HG/SGCH00.mspx

### A fiókzárolási házirend meghatározása

A fiókzárolási házirend meghatározásakor járjon el körültekintően. Kisvállalkozások esetén ezt a házirendet nem szabad beállítani, mert nagy valószínűséggel kizárhat hitelesített felhasználókat is, ez pedig rendkívüli költségekkel járhat az ügyfél részéről.

Ha az ügyfél fiókzárolási házirend bevezetése mellett dönt, állítsa a **Fiókzárolás küszöbe** beállítást elegendően nagy értékre ahhoz, hogy a hitelesített felhasználók ne zárják ki magukat a jelszó többszöri elgépelése miatt.

A fiókzárolási házirenddel kapcsolatban további tájékoztatást a Windows Server súgójának „Fiókzárolási házirend – áttekintés” című témakörében találhat.

A fiókzárolási házirend alkalmazásával vagy módosításával kapcsolatban további tájékoztatást a Windows Server súgójának „A fiókzárolási házirend alkalmazása vagy módosítása” című témakörében találhat.

## Hozzáférés-vezérlés

A Windows hálózat és erőforrásai (például a Navision program) biztonságossá tételéhez figyelembe kell venni, hogy a felhasználók, felhasználói csoportok és számítógépek milyen hálózati jogokkal rendelkeznek. A számítógépek biztonsága azáltal szabályozható, hogy felhasználóik meghatározott jogokat kapnak. Az objektumok, például fájlok vagy mappák biztonsága azáltal szabályozható, hogy engedélyeket rendelünk hozzájuk, amelyek révén a felhasználók vagy csoportok meghatározott műveleteket végezhetnek velük. A hozzáférés-vezérlés alapfogalmai a következők:

- Engedélyek
- Objektumok tulajdonosi joga
- Engedélyek öröklődése

- Felhasználói jogok
- Objektumnaplózás

## Engedélyek

Az engedélyek szabják meg, hogy a felhasználók vagy csoportok milyen hozzáféréssel rendelkeznek az objektumokhoz és tulajdonságaikhoz, például fájlokhoz, mappákhoz vagy a rendszerleíró adatbázis objektumaihoz. Engedély bármilyen biztonságos objektumhoz, például fájlhoz vagy rendszerleíró objektumhoz rendelhető. Az engedélyeket felhasználóknak, csoportoknak vagy számítógépeknek lehet megadni. A csoportos engedélyek használata a legcélszerubb.

## Objektumok tulajdonosi joga

Az objektumhoz létrehozáskor a rendszer tulajdonost rendel. Windows 2000 Server rendszerben az objektum alapértelmezett tulajdonosa a létrehozó. Windows Server 2003 rendszerben a Rendszergazdák csoport tagjai által létrehozott objektumok esetében ez másképp van:

itt a Rendszergazdák csoport lesz a tulajdonos, nem pedig az objektumot létrehozó személy. Ez a szabály a Microsoft Management Console (MMC) Helyi biztonsági beállítások beépülő moduljában módosítható, a **Rendszerobjektumok: A Rendszergazdák csoport tagjai által létrehozott objektumok alapértelmezett tulajdonosa** beállítással. Az objektumon beállított engedélyeket a tulajdonos bármikor módosíthatja.

További tájékoztatást a Windows Server súgójának „Tulajdoni jog” című témakörében találhat.

## Engedélyek öröklődése

Az öröklődés segítségével a rendszergazdák egyszerűen oszthatják ki és kezelhetik az engedélyeket. A valamely tárolóban lévő objektumok automatikusan öröklik a tároló örökölhető tulajdonságait. A valamely mappában létrehozott fájlok például öröklik a mappa engedélyeit, de csak az örökölhetőként megjelölt engedélyeket.

## Felhasználói jogok

A felhasználói jogok meghatározott jogosultságokat és bejelentkezési jogokat adnak a környezet felhasználóinak és csoportjainak.

További tájékoztatást a Windows Server súgójának „Felhasználói jogok” című témakörében találhat.

## Objektumnaplózás

Naplózhatja a felhasználók objektumokhoz való hozzáférését. Ezek a biztonsággal kapcsolatos események az Eseménynapló biztonsági naplójában találhatók meg.

További tájékoztatást a Windows Server súgójának „Naplózás” című témakörében találhat.

### Hozzáférés-vezérlés – gyakorlati tanácsok

- Az engedélyeket ne felhasználókhoz, hanem csoportokhoz rendelje. Mivel a felhasználói fiókok egyéni kezelése kevéssé hatékony, felhasználónként csak kivételes esetben érdemes engedélyt kiadni.
- Bizonyos esetekben célszerű az engedélyeket megtagadni, például amikor egy engedéllyel rendelkező csoport egy részének hozzáférését szeretné visszavonni.
- Soha ne tagadja meg egy objektum elérését a Mindenki csoporttól. Ez a tilalom ugyanis a rendszergazdákra is vonatkozik. Célszerűbb ilyen esetben eltávolítani a Mindenki csoportot, és a többi felhasználó, csoport és számítógép engedélyeit beállítani. Ne feledje, hogy ha nem ad meg semmilyen engedélyt, akkor senki nem fér az objektumhoz.
- Az objektumok engedélyeit a fa lehető legmagasabb szintjén állítsa be, majd örökítse a biztonsági engedélyeket az alsóbb szintekre. A hozzáférés-vezérlési beállításokat gyorsan és hatékonyan örökítheti a szülőobjektum alatti részfára. Így érheti el a legjobb eredményt a legkisebb ráfordítással. A kialakított engedélyek a felhasználók, csoportok és számítógépek többségének megfelelőek lesznek.
- Az explicit engedélyek felülbírálják az örökölteket. Az örökölt engedély-megtagadást például felülbírálja az objektum explicit hozzáférési engedélye. Az explicit engedélyek tehát előbbrevalók az örökölt engedélyeknél és engedély-megtagadásoknál.
- Az Active Directory® objektumok engedélyeivel kapcsolatban tekintse át az ezekre vonatkozó gyakorlati tanácsokat.

További tájékoztatást a Windows Server súgójának „Engedélyek hozzárendelése Active Directory objektumokhoz – gyakorlati tanácsok” című témakörében találhat.

## Külső biztonság: tűzfal

A tűzfal olyan szoftver- vagy hardvereszköz, amely megakadályozza egyes adatcsomagok adott hálózatról való ki- vagy oda történő belépését. A forgalom szabályozása úgy történik, hogy a tűzfal egyes portjai vagy engedélyezik, vagy meggátolják az adatcsomagok áthaladását. A tűzfal az adatcsomagok több adatát is vizsgálja: a csomagot továbbító protokollt, a csomag feladóját és címzettjét, a csomag tartalmának típusát, és a cél portszámát. Ha a tűzfalnak engedélyezték az adott protokoll fogadását az adott porton, a csomag átmehet. A Microsoft Windows Small Business Server 2003 Premium Edition a Microsoft Internet Security and Acceleration (ISA) Server 2000 programot tartalmazza tűzfalként. A Small Business Server Standard Edition is rendelkezik tűzfallal.

# ISA Server 2004

Az Internet Security and Acceleration (ISA) Server 2000 biztonságosan irányítja az internet és a belső hálózat ügyfélgépei közötti kéréseket és válaszokat.

Az ISA Server biztonságos átjáróként muködik a helyi hálózat ügyfélgépei számára. A programot futtató számítógép transzparens a kommunikációs útvonal többi eleme számára. Az internetes felhasználó nem észleli a tuzfalkiszolgáló jelenlétét, amíg olyan szolgáltatást vagy webhelyet nem próbál elérni, melyet az ISA Server megtagad. Az elért internetes kiszolgáló úgy értelmezi a programot futtató számítógép kéréseit, mintha azok az ügyfélalkalmazástól származnának.

IP-töredékszűrés esetén a webes proxy- és tűzfalszolgáltatások szűrik a töredékcsomagokat. Ezáltal a hiányos IP-csomagokat a rendszer eldobja. Az egyik bevett támadási forma lényege, hogy töredezett IP-csomagokat küldenek a számítógépre, majd a rendszerre ártalmas módon állítják össze a töredékeket.

Az ISA Server rendelkezik behatolás-észlelő mechanizmussal, feljegyzi a behatolási kísérletek időpontját, és végrehajtja az előre meghatározott muveleteket vagy riasztásokat.

Ha az Internet Information Services (IIS) program telepítve van az ISA Server számítógépére, akkor be kell állítani, hogy ne használja azon portokat, melyeken az ISA Server a kimenő webes kéréseket küldi (alapértelmezés: 8080) és a bejövő kéréseket fogadja (alapértelmezés: 80). Megadhatja például, hogy az IIS a 81-es portot figyelje, majd beállíthatja, hogy az ISA Server a bejövő webes kéréseket az IIS-t futtató helyi számítógép 81-es portjára továbbítsa.

Ha az ISA Server és az IIS által használt portok ütköznek, a telepítő leállítja az IIS közzétételi szolgáltatását. Ilyenkor adja meg az IIS-nek, hogy más portot figyeljen, majd indítsa újra a közzétételi szolgáltatást.

### Az ISA Server házirendjei

Meghatározhatja a bejövő és kimenő forgalmat szabályozó ISA Server házirendet. A hely- és tartalmi szabályok határozzák meg, hogy mely helyek és tartalmak érhetők el. A protokollszabályok jelzik, hogy az egyes protokollok elérhetők-e a kimenő vagy a bejövő forgalom számára.

Létrehozhat tartalmi és helyszabályokat, protokollszabályokat, webes közzétételi szabályokat és IP-csomagszűrőket. Ezek a házirendek határozzák meg, hogyan kommunikálnak az ISA Server ügyfelei az internettel, és hogy a kiszolgáló milyen kommunikációt engedélyez.

## Vírusvédelem

A számítógépes vírus olyan végrehajtható fájl, amely önmaga sokszorosítására vagy elrejtésére, illetve adatok és programok törlésére vagy rongálására fejlesztettek ki. A vírusokat gyakorta átírják vagy átalakítják, hogy észlelésüket megnehezítsék. A vírusok sokszor e-mailek mellékleteként terjednek. A vírusellenőrző programokat folyamatosan frissíteni kell, hogy az új és átalakított vírusokat is észleljék. A vírusok a számítógépes rongálás elsődleges eszközei.

A vírusellenőrző szoftvereket kimondottan a vírusok felismerésére és elhárítására fejlesztik. Mivel folyamatosan születnek új vírusok, számos vírusellenőrző termék gyártója rendszeres frissítéseket kínál vásárlóinak.

A Microsoft erősen ajánlja, hogy ügyfelei használjanak vírusellenőrző programokat.

Ezeket általában három helyre telepítik: a felhasználói munkaállomásokra, a kiszolgálókra, és a szervezet e-mail forgalmát lebonyolító hálózatra.

## A vírusok fajtái

A számítógépes rendszereket megfertőző vírusoknak három főbb fajtája van: a rendszerindító szektort és a fájlokat fertőző vírusok, illetve a trójai programok.

### A rendszerindító szektort fertőző vírusok

Amikor a számítógép elindul, az operációs rendszer vagy bármilyen indítófájl betöltése előtt beolvassa a merevlemez rendszerindító szektorát. Ezek a vírusok saját kódjukkal töltik fel a rendszerindító szektort. Ha a számítógép ilyen vírussal fertőződik meg, indításkor a vírus kódja kerül először a memóriába. Ezután a vírus a fertőzött gép által használt lemezeken sokszorosíthatja magát.

### Fájlokat fertőző vírusok

A vírusok leggyakoribb fajtájának tagjai végrehajtható programfájlokhoz fűzik saját kódjukat. A víruskód általában észrevétlenül kerül a programba. A fertőzött fájl futtatásakor a vírus más fájlokhoz is csatolhatja magát. Az ilyen vírusok által fertőzhető fájlok általában .com, .exe vagy .sys kiterjesztésűek.

Egyes fájlfertőző vírusokat adott programtípusokhoz fejlesztenek. Gyakori célpontot jelentenek az .ovl és .dll fájlok. Bár ezek önmagukban nem futtathatók, más programok meghívják ezek kódját, és ilyenkor a vírus is továbbterjedhet.

Az adatok akkor károsodnak, amikor a vírus működésbe lép. Ez történhet a fertőzött fájlok futtatásakor vagy valamilyen rendszerkörülménnyel kapcsolatos feltétel teljesülésekor (például adott rendszerdátum napján).

### Trójai programok

A trójai programok valójában nem vírusok. A két típus közti alapvető különbség az, hogy a trójai program nem sokszorosítja önmagát, hanem a merevlemez adatait károsítja. A trójai általában valamilyen hasznos programnak álcázza magát, például játéknak vagy segédprogramnak. Futtatáskor azonban törölheti vagy károsíthatja az adatokat.

## Vírusvédelem – gyakorlati tanácsok

A makróvírusok terjedése megállítható. Az alábbi kapcsolódó javaslatokat ossza meg ügyfeleivel:

- Telepítsen olyan vírusellenőrző megoldást, amely a bejövő üzeneteket még az útválasztó előtt ellenőrzi, így az e-mailekben is felfedezi az ismert vírusokat.
- Ellenőrizze a kapott dokumentumok forrását. Ne nyisson meg semmilyen dokumentumot, amíg nem győződött meg róla, hogy megbízható forrásból származik.
- Lépjen kapcsolatba a dokumentum szerzőjével. Ha a felhasználók bizonytalanok a dokumentum biztonságával kapcsolatban, keressék meg annak szerzőjét.
- Használja a Microsoft Office makróvírus-védelmét. Az Office alkalmazások figyelmeztetik a felhasználót, ha a dokumentum makrókat tartalmaz. Így a felhasználók dönthetik el a dokumentum megnyitásakor, hogy engedélyezik-e a makrókat.
- A makróvírusok észlelésére és eltávolítására használjon vírusellenőrző programot. A vírusellenőrzők észlelik, és gyakorta el is távolítják a makróvírusokat a dokumentumokból. A Microsoft az International Computer Security Association (ICSA) nemzetközi biztonsági szervezet által minősített vírusellenőrzőket ajánlja.

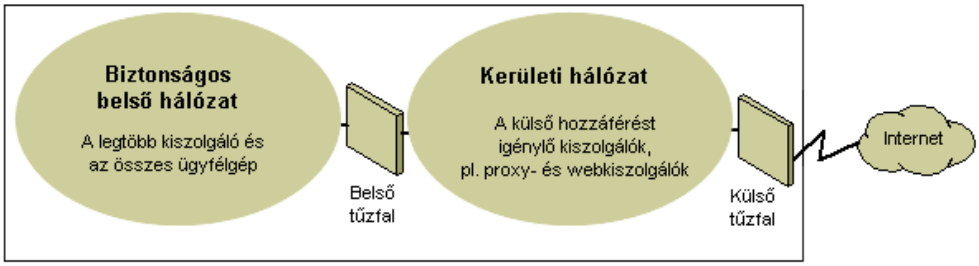
A vírusokkal és általában a számítógépes biztonsággal kapcsolatban további tájékoztatást találhat a következő webhelyeken:

- Microsoft Security: http://www.microsoft.com/security/default.asp
- A Microsoft TechNet biztonsági dokumentumai: http://www.microsoft.com/technet/security/Default.mspx

# Hálózati biztonsági stratégiák

Mivel az IP-hálózati környezet megtervezése és kialakítása a magán- és nyilvános hálózatok szempontjainak figyelembevételét egyaránt igényli, a tűzfal a hálózati biztonság kulcseleme lett. A tűzfal nem feltétlenül egyetlen összetevő. A National Computer Security Association (NCSA) nevű szervezet így definiálja a tűzfalat: „két vagy több hálózat között határként funkcionáló rendszer vagy rendszerek összessége”. Bár különféle megnevezések vannak használatban, ezt a határt gyakran hívják kerületi hálózatnak (perimeter network). A kerületi hálózat védi az intranetet vagy a vállalati hálózatot az internetről vagy más nagy hálózatokról érkező behatolási kísérletektől.

Az alábbi ábra egy tűzfalakkal határolt kerületi hálózatot mutat be, amelyet védelmi célból egy magánhálózat és az internet közé helyeztek:




**Alapvető kerületi hálózat**

Az egyes szervezetek különféle módokon használják a tűzfalakat. Az IP-csomagszűrés gyenge védelmet nyújt, könnyű megkerülni, és kezelése nehézkes. Az alkalmazásátjárók biztonságosabbak, mint a csomagszűrők, és kezelésük is egyszerűbb, mert csak bizonyos alkalmazásokat, például egy adott levelezőprogramot kell kezelniük. Az áramköri átjárók akkor

a leghasznosabbak, ha valamely hálózati alkalmazás felhasználója nagyobb problémát jelent, mint az alkalmazás által továbbított adatok. A proxykiszolgáló átfogó biztonsági eszköz, amely alkalmazásátjárót tartalmaz, és többek között biztonságos hozzáférést nyújt névtelen felhasználóknak is. Most a fenti lehetőségekről olvashat kicsit bővebben:

- **IP-csomagszűrés**
  Az IP-csomagszűrés volt a tűzfal-technológia első állomása. A program a csomagfejlécekben többek közt ellenőrzi a forrás és a cél címét, illetve a TCP és UDP portszámot.
  A csomagszűrés lehetőségei korlátozottak, és leginkább egyszerű biztonsági környezetekben használható, ahol a kerületi hálózaton kívül semmi nem megbízható, belül pedig minden az. Az utóbbi években több gyártó is intelligens döntéshozatali szolgáltatásokkal fejlesztette tovább a csomagszűrést. Ezt az új technológiát *állapot-nyilvántartásos protokollvizsgálatnak (stateful protocol inspection)* nevezik. A csomagszűrés beállítható úgy, hogy egyes csomagtípusokat elfogadjon, és az összes többit visszautasítsa, vagy fordítva.
- **Alkalmazásátjárók**
  Az alkalmazásátjárókat akkor használják, ha az alkalmazás tartalma okozza a legnagyobb problémát. Legnagyobb erősségük és korlátjuk egyaránt az, hogy adott alkalmazásokhoz készülnek, így a technológiai változásokhoz nehezen idomulnak.
- **Áramköri átjárók**
  Az áramköri átjárók a tűzfalba épített alagutak, amelyek egyes folyamatokat vagy rendszereket kötnek össze a tűzfalon keresztül. Ezek használata akkor célszerű, ha az alkalmazást használó személy nagyobb kockázatot jelent, mint az alkalmazás által továbbított adatok. Az áramköri átjáró abban különbözik a csomagszűrőtől, hogy képes további adatokat szolgáltató, közvetlenül csatlakoztatott alkalmazássémához kapcsolódni.
- **Proxykiszolgálók**
  A proxykiszolgáló átfogó biztonsági eszköz, amely a helyi hálózat és az internet közti forgalmat szabályozó tűzfal- és alkalmazásátjáró-szolgáltatásokat nyújt.
  A proxykiszolgálók képesek dokumentum-gyorsítótárazásra és hozzáférés-vezérlésre is. Teljesítményük növelhető a gyakran lekért adatok, például népszerű weblapok gyorsítótárazásával. A proxykiszolgálók szűrik és visszautasítják azokat a kéréseket, amelyeket a tulajdonos nem talál megfelelőnek, például a bizalmas fájlokhoz való illetéktelen hozzáférési kísérleteket.

Gondoskodjon róla, hogy ügyfele igénybe vegye a tűzfalak által nyújtott, számára hasznos biztonsági szolgáltatásokat. Helyezzen külső tűzfallal fenntartott kerületi hálózatot a hálózati topológia azon pontjára, ahol a vállalati hálózaton kívülről érkező adatforgalom egésze áthalad. A tűzfal hozzáférés-vezérlését az ügyfél igényei szerint állíthatja be, és megszabhatja, hogy a tűzfal minden jogosulatlan hozzáférési kísérletet jelentsen.

Annak érdekében, hogy a belső tűzfalon csak a mindenképp szükséges portokat kelljen megnyitni, használjon alkalmazásszintű tűzfalat, például az ISA Server 2000 programot.

A TCP/IP protokollal kapcsolatban további tájékoztatást a "Designing a TCP/IP Network" (TCP/IP-hálózatok tervezése) című webhelyen találhat: http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dnsbb_tcp_overview.asp

## Vezeték nélküli hálózatok

A vezeték nélküli hálózatok alapbeállításai általában lehetőséget adnak a jelek lehallgatására. Bizonyos vezeték nélküli hálózati eszközök alapbeállításai, az ilyen hálózatok egyszerű elérhetősége és a jelenlegi titkosítási technikák miatt

fokozottan ki vannak téve a behatolóknak. Vannak olyan beállítások és eszközök, amelyekkel a hallgatózás meggátolható, de ne feledje, hogy ezek nem védik a számítógépeket az internetkapcsolaton keresztül érkező betörőktől és vírusoktól. Ezért rendkívül fontos, hogy tűzfallal tartsa távol a nem kívánt internetes betörőket.

A vezeték nélküli hálózatok védelmével kapcsolatban a „How to Make Your 802.11b Wireless Home Network More Secure" (802.11b típusú vezeték nélküli hálózatokkal kapcsolatos biztonsági tanácsok) című cikkben találhat további tájékoztatást: http://support.microsoft.com/default.aspx?scid=kb;en-us;309369

## Hálózati biztonsági forgatókönyvek

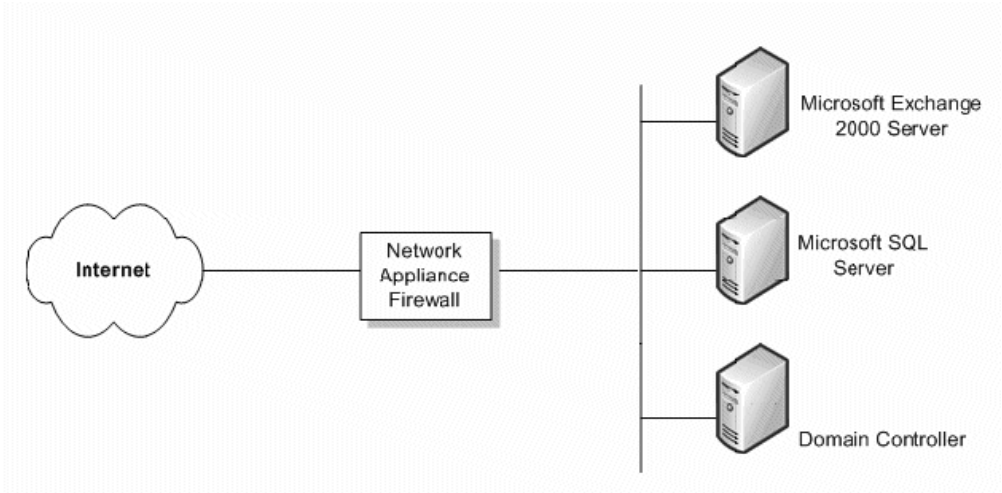
Az ügyfél által elvárt hálózati biztonsági szint több tényezőtől függ. A leggyakoribb a költségvetés lehetőségei és a vállalati adatbiztonság követelményei közti kompromisszum. Kisvállalatok is rendelkezhetnek a legszilárdabb védelmet nyújtó összetett biztonsági megoldásokkal, de ritkán engedhetik meg maguknak ezeket. Ebben a szakaszban négy lehetséges esetet tekinthet át a kapcsolódó javaslatokkal együtt.

### Nincs tűzfal

Ha az ügyfél rendelkezik internetkapcsolattal, de tűzfallal nem, akkor biztonsági intézkedésekre van szükség. Az egyszerűbb tűzfalkészülékek is elegendő védelmet nyújtanak a legtöbb amatőr betörő ellen.

### Egy egyszerű tűzfal

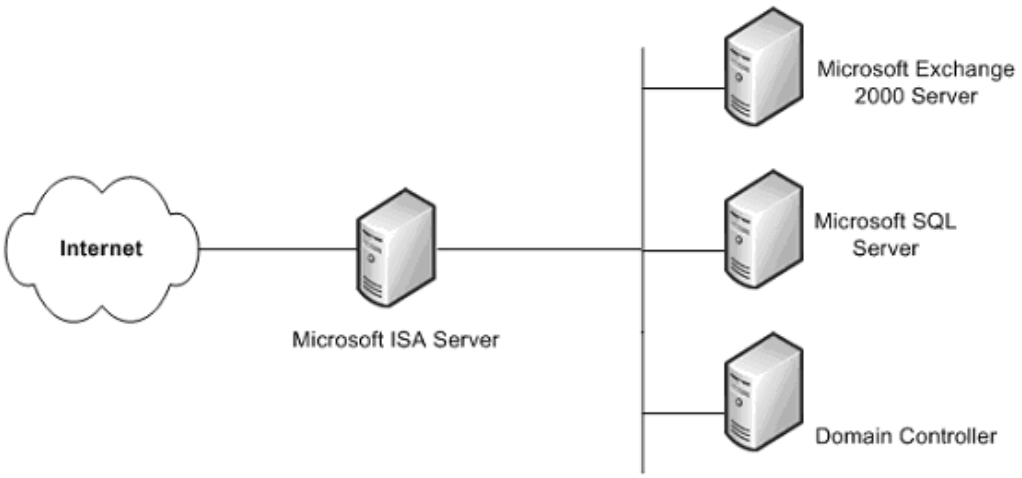
Az internet és az ügyfél adatai között a minimális ajánlott biztonsági felszerelés egy tűzfal. Ez nem feltétlenül nyújt kifinomult védelmet, így nem tekinthető nagyon biztonságosnak, de a semminél jobb.




**Egyszerű tűzfal**

Az ügyfél adatainak védelmében remélhetőleg megengedheti magának a biztonságosabb megoldásokat. Az egyik ilyen megoldás az ISA Server. A kiszolgáló a költség ellenében sokkal megbízhatóbb védelmet nyújt, mint az

átlagos tűzfalak, mivel azok általában csak csomagszűrést és hálózati címfordítást (NAT) szolgáltatnak.




**Tűzfal ISA Server kiszolgálóval**

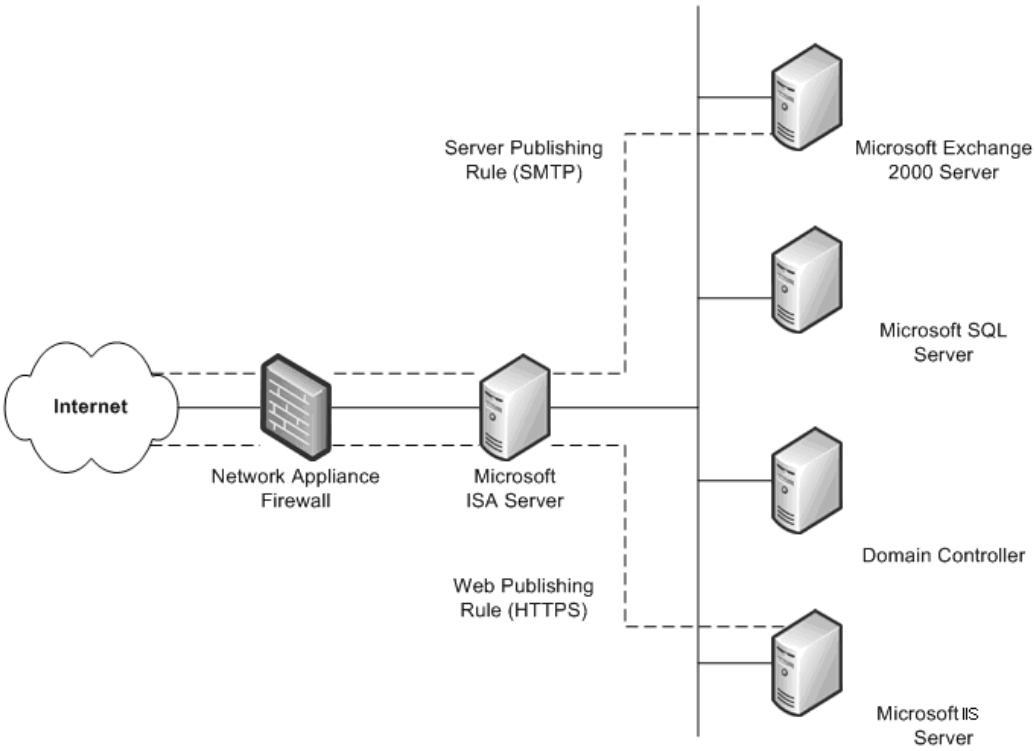
Ez az egytűzfalas megoldás biztonságosabb, mint az alsó kategóriás tűzfalkészülékek, és a Windows rendszerre tervezett biztonsági megoldásokat nyújt.

## Egy meglévő tűzfal

Ha az ügyfél már rendelkezik az intranetet az internettől elválasztó tűzfallal, akkor célszerű emellé egy másikat üzembe helyezni, így a belső erőforrások többféleképpen is beállíthatók.

Az egyik ilyen módszer a webes közzététel. Ilyenkor egy ISA Server kiszolgálót telepítenek a szervezet internetes felhasználók számára hozzáférést nyújtó webkiszolgálója elé. A bejövő webes kérésekkel szemben az ISA Server kifelé webkiszolgálóként viselkedik, az ügyfélkérésekre a saját gyorsítótárából származó webtartalmat küldi el, és csak akkor továbbítja a kérést a webkiszolgáló felé, ha a gyorsítótárból nem tudja teljesíteni.

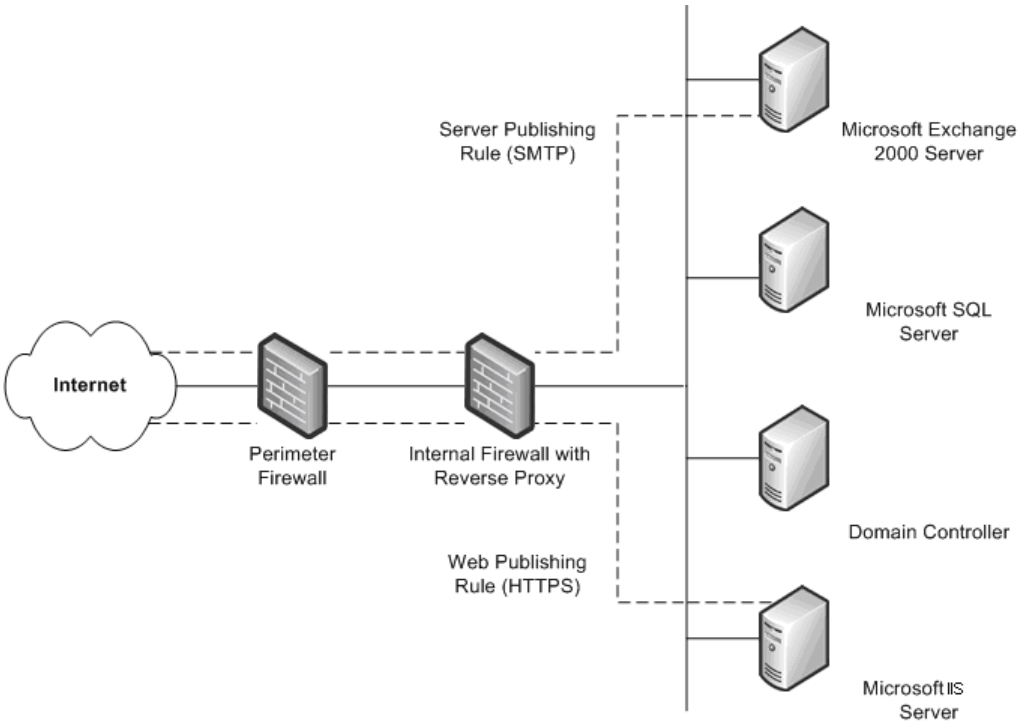
A másik módszer a kiszolgáló-közzététel. Az ISA Server a belső kiszolgálók számára lehetővé teszi az internet felé irányuló közzétételt anélkül, hogy a belső hálózat biztonságát veszélyeztetnék. A webes és a kiszolgáló-közzététel szabályai határozzák meg, hogy mely kérések kerülnek a helyi hálózat valamely kiszolgálójához, és ez további biztonsági réteget képez a belső kiszolgálók számára.




**Meglévő tűzfal és hozzákapcsolt ISA Server kiszolgáló**

## Két meglévő tűzfal

A negyedik esetben a szervezetnél már két tűzfal üzemel, és létezik a kerületi hálózat (DMZ). Ezen kiszolgálók egyike fordított proxyszolgáltatást nyújt, hogy az internetes ügyfelek ne érjék el közvetlenül az intranetes kiszolgálókat. Ehelyett az egyik (ideális esetben a belső) tűzfal elfogja a belső kiszolgálók felé irányuló kéréseket, megvizsgálja ezeket a csomagokat, és utána az internetes állomás nevében továbbítja azokat.




**Két meglévő tűzfal**

Ez az eset hasonló az előző kimeneteléhez (a második tűzfal hozzáadása után). Az egyetlen különbség az, hogy a fordított proxyszolgáltatást nyújtó belső tűzfal nem ISA Server. Ebben az esetben az Ön feladata a tűzfalak rendszergazdáival együtt a biztonsági házirendnek megfelelően meghatározni a kiszolgálók közzétételi szabályait.

## Biztonsági javítások kezelése

Az operációs rendszerek és alkalmazások gyakran rendkívül bonyolult programok. Az akár több millió sornyi kódot sok programozó készíti el. Létfontosságú, hogy a szoftver megbízhatóan muködjön és ne veszélyeztesse a számítástechnikai környezet biztonságát és stabilitását. A problémák elkerülése érdekében a programokat kiadás előtt tesztelik. A támadók azonban folyamatosan kutatják a szoftverek gyenge pontjait, így nem lehet előre felkészülni minden jövőbeli támadásra.

A biztonsági javítások kezelése számos szervezet esetében része az általános változás- és konfigurációkezelési stratégiának. Bármilyen és bármekkora szervezetről legyen is szó azonban, létfontosságú, hogy megfelelő biztonsági javítási stratégiával rendelkezzen, még ha változás- és konfigurációkezelést nem is folytat. A számítógépes rendszereket érő sikeres támadások túlnyomó többsége azért sikeres, mert a biztonsági javításokat nem telepítették.

A biztonsági javítások külön kihívást jelentenek a legtöbb szervezetnek. Ha a szoftver egy gyenge pontját felfedezik, a hackerközösségben gyorsan elterjed az információ. Ilyenkor a Microsoft igyekszik a lehető legrövidebb időn belül közzétenni a javítást. A közzétételig az ügyfelek biztonsága ugyanis súlyos csorbát szenved.

Navision környezetben is gondoskodni kell róla, hogy ügyfelei teljes rendszerén telepítve legyenek a legfrissebb biztonsági javítások. Ellenőrizze, hogy az ügyfél a Microsoft által rendelkezésre bocsátott technológiák valamelyikét használja. Ezek a következők:

- **Microsoft Security Notification Service**
  A Security Notification Service biztonsági értesítőszolgáltatás egy e-mail lista, amely értesítést küld az új frissítések megjelenéséről. Ezek az értesítések értékes elemét képezhetik a proaktív biztonsági stratégiának. Elérhetők a TechNet Product Security Notification webhelyen is:
  http://www.microsoft.com/technet/security/bulletin/notify.mspx
- **Automatikus frissítések**
  A Windows automatikusan is képes telepíteni a biztonsági frissítéseket.
- **Microsoft Security Bulletin keresőeszköz**
  A Security Bulletin keresőeszköz a Security Bulletin webhelyén érhető el: http://www.microsoft.com/technet/security/current.aspx. Segítségével az ügyfél meghatározhatja, hogy mely frissítésekre van szüksége a használt operációs rendszer, alkalmazások és szervizcsomagok alapján.
- **Microsoft Baseline Security Analyzer (MBSA)**
  Ez a grafikus eszköz a Microsoft Baseline Security Analyzer webhelyen érhető el: http://www.microsoft.com/technet/security/tools/mbsahome.mspx. A program a Microsoft által fenntartott javítási listával hasonlítja össze a számítógép állapotát. Az MBSA alapvető biztonsági ellenőrzéseket is végez, többek közt a jelszavak erősségét, lejárati beállításait, a vendégfiók-házirendeket illetően. Az MBSA ezen kívül megvizsgálja a Microsoft Internet Information Services (IIS), SQL Server™ 2000, Exchange 5.5, Exchange 2000 és Exchange Server 2003 programokat is.
- **Microsoft Software Update Services (SUS)**
  A korábban Windows Update Corporate Edition néven ismert szolgáltatás segítségével a nagyvállalatok helyi számítógépeken tárolhatják a nyilvános Windows Update webhelyen is megtalálható kritikus frissítéseket és SRP csomagokat. Az eszköz az automatikus frissítéshez használt ügyfélprogram új verziójának köszönhetően hatékony automatikus letöltési és telepítési modellt biztosít. Az új ügyfélprogram Windows 2000 és Windows Server 2003 operációs rendszerekhez használható, és képes automatikusan telepíteni a letöltött frissítéseket. A Microsoft SUS szolgáltatásról a következő webhelyen találhat további tájékoztatást:
  http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp
- **Microsoft Systems Management Server (SMS) Software Update Services Feature Pack**
  A SMS szoftverfrissítési csomagja számos, a szoftverfrissítések vállalati kezelését megkönnyítő eszközt tartalmaz. Ezek között megtalálhatók a biztonsági frissítéseket nyilvántartó eszközök, egy szoftverfrissítéseket terjesztő varázsló, és az SMS webes jelentéskészítő eszköze a szoftverfrissítésekhez használható webes jelentéskészítő bővítménnyel. Ezekrol az eszközökről a következő webhelyen találhat további tájékoztatást: http://www.microsoft.com/smserver/downloads/20/featurepacks/suspack/

Ismertesse ügyfeleivel ezeket az eszközöket, és ösztönözze őket használatukra. Rendkívül fontos, hogy a biztonsági problémákat minél hamarabb elhárítsák, és fenntartsák a környezet stabilitását.

# Az SQL Server 2000 biztonsági beállításai

Mivel a Navision SQL Server 2000 kiszolgálón is fut, fontos, hogy az ügyfél SQL Server 2000 kiszolgálójának biztonságát is szavatolják. Ebben segíthetnek a következő intézkedések:

- Gondoskodjék róla, hogy az operációs rendszer és az SQL Server 2000 legújabb szervizcsomagjai és frissítései telepítve legyenek. Ezzel kapcsolatban részleteket a Microsoft Security webhelyen olvashat: http://www.microsoft.com/security/default.asp
- A fájlrendszer-szintű biztonság érdekében ellenőrizze, hogy az SQL Server 2000 összes adat- és rendszerfájlja NTFS-partícióra van telepítve. A fájlokhoz csak rendszergazdai vagy rendszerszintű felhasználóknak biztosítson hozzáférést az NTFS engedélyeivel. Ezzel védelmet biztosít azon felhasználók ellen, akik az MSSQLSERVER szolgáltatás leállítása után próbálják meg elérni a fájlokat.
- Az SQL Server 2000 szolgáltatáshoz (MSSQLSERVER) használjon alacsony jogosultsági szinttel rendelkező tartományi fiókot, például az NT Authority\Hálózatszolgáltatás vagy a LocalSystem fiókot (utóbbi ajánlott). A fióknak csak a mindenképpen szükséges jogosultságokat adja meg a tartományban. Ezzel segíthet feltartóztatni a kiszolgálót érő támadást. A fióknak tehát csak helyi felhasználói szintű engedélyeket adjon. Ha az SQL Server 2000 tartományi rendszergazdafiókból futtatja a szolgáltatásokat, a kiszolgálót ért támadás az egész tartományra kihathat. A beállítást az SQL Server Enterprise Manager segítségével módosíthatja. A fájlok, a rendszerleíró adatbázis és a felhasználói jogok hozzáférés-vezérlési listái ezután automatikusan módosulnak.
- Az SQL Server 2000 legtöbb kiadása két alapértelmezett adatbázissal kerül telepítésre (a **Northwind** és a **pubs** nevűekkel). Mindkettő tesztelésre, oktatásra és általános példák bemutatására készült mintaadatbázis. Üzleti környezetben ezek telepítése nem ajánlott. Az adatbázisok jelenléte az alapbeállítások gyenge pontjainak kihasználásán alapuló támadásra bátoríthat. Ha a **Northwind** és **pubs** adatbázisok megtalálhatóak az SQL Server 2000 számítógépen, távolítsa el azokat.
- Az SQL Server 2000 rendszer naplózása alapértelmezés szerint nem engedélyezett, így a feltételeket a rendszer nem naplózza. Ez megnehezíti a behatolások észlelését, és megkönnyíti a támadók számára nyomaik eltüntetését. Mindenképpen engedélyezze legalább a sikertelen bejelentkezések naplózását.

Az SQL Server 2000 legfrissebb biztonsági információit a következő webhelyen találhatja: http://www.microsoft.com/sql/techinfo/administration/2000/security/default.asp

# Bemutatkozik a Microsoft Business Solutions

A Microsoft Business Solutions, a Microsoft leányvállalata integrált üzleti alkalmazásokat és szolgáltatásokat kínál, amelyek megkönnyítik a kis-, közép- és nagyvállalatok számára a megrendelőikkel, beszállítóikkal, üzletfeleikkel és alkalmazottaikkal való kapcsolattartást. A Microsoft Business Solutions alkalmazásai a pénzügyek, elemzések, az emberierőforrás-kezelés, a projektmenedzsment, az ügyfélkapcsolat-kezelés, a helyszíni szolgáltatások, az ellátásilánc-kezelés, az e-kereskedelem, a gyártás és a készletezés stratégiai üzleti folyamatait optimalizálják. Az alkalmazások hozzájárulnak megrendelőink üzleti sikeréhez. A Microsoft Business Solutions céggel kapcsolatban további tájékoztatást a következő webhelyen találhat: http://www.microsoft.com/BusinessSolutions/

Ez a dokumentum nem végleges, így a vonatkozó szoftvertermék kereskedelmi forgalomba hozatala elott a szöveg lényegesen változhat.

A dokumentumban foglaltak a Microsoft Corporation vonatkozó problémákkal kapcsolatos, a kiadás idopontjában érvényes véleményét tükrözik. Mivel a Microsoft tevékenységére kihatnak a változó piaci feltételek, a szöveg nem értelmezheto a Microsoft kötelezettségvállalásaként, és a Microsoft a kiadás idopontja után nem vállal felelosséget az információk pontosságáért.

Ez a sokumentumtervezet kizárólag tájékoztatási célokat szolgál. A MICROSOFT SEMMILYEN JÓTÁLLÁST NEM VÁLLAL A DOKUMENTUM RÉVÉN.

A kapcsolódó szerzoi jogszabályok betartása a felhasználó felelőssége. A szerzői jogok korlátozása nélkül a dokumentum egyetlen része sem másolható, és a dokumentum nem rögzíthető és nem tárolható visszakereshető rendszerben. Továbbítása semmiféle formában és semmilyen módon (elektronikus, mechanikai, fénymásolás, hangrögzítési vagy más eljárással) vagy célból nem engedélyezett. Ehhez a Microsoft Corporation írásban rögzített engedélye szükséges.

A Microsoft a dokumentumban foglaltakkal kapcsolatban szabadalmakkal, szabadalmi beadványokkal, védjegyekkel, szerzői jogokkal vagy más szellemi tulajdonjogokkal rendelkezhet. A jelen dokumentum szövegezése a felhasználót e szabadalmakra, védjegyekre, szerzői jogokra és más szellemi tulajdonjogokra vonatkozóan semmiféle licencjoggal nem ruházza fel, hacsak a Microsofttal kötött valamely írásbeli licencszerződés kifejezetten nem biztosít ilyen jogokat.

© 2003 Microsoft Business Solutions ApS, Dánia. Minden jog fenntartva.

A Microsoft, a Great Plains és a Navision a Microsoft Corporation, a Great Plains Software, Inc vagy a Microsoft Business Solutions ApS vagy leányvállalataik védjegyei vagy bejegyzett védjegyei az Amerikai Egyesült Államokban, illetve más országokban. A Great Plains Software, Inc. és a Microsoft Business Solutions ApS a Microsoft Corporation leányvállalatai. A jelen dokumentációban megemlített tényleges vállalat- és terméknevek jogtulajdonosaik bejegyzett védjegyei. A példákban fiktív vállalatok, szervezetek, termékek, tartománynevek, e-mail címek, emblémák, személyek és események szerepelnek. Bármely létező céggel, szervezettel, termékkel, tartománynévvel, e-mail címmel, emblémával, személlyel vagy eseménnyel való esetleges egyezés csak véletlenül fordulhat elő, a szándékosság ki van zárva.