

1 Kisiroda internet-hozzáféréssel

Ez a könyv a Windows Server 2008 operációs rendszerről szól, amely kiszolgálókat működtet – és gyakorlatilag bárhol használható, a legkisebbtől a legnagyobb hálózatiig. Könyvünkben öt felhasználási helyet mutatunk be, leírva, hogy a Windows Server 2008 melyikben hogyan, milyen beállításokkal alkalmazható.

Elsőként egy olyan irodát veszünk alapul, amelyben tízen-tizenötven dolgoznak – tulajdonképpen nem is érdekes, hogy mivel, elég azt feltételezni, hogy mindannyian „tudásmunkások”¹, akik a munkájuk java részét számítógépen végzik, anélkül hogy informatikusok lennének. Beszélhetünk lapkiadóról, építészirodáról vagy éppen ügyvédi vagy közjegyzői irodáról.

A tudásmunkások dokumentumokkal – szövegekkel, táblázatokkal, képekkel, bemutatókkal, tervrajzokkal stb. – dolgoznak. Egy dokumentum a számítógépen egy vagy több fájl formájában jelenik meg.

Ha egy irodában többen dolgoznak, feltételezhetjük, hogy azt együtt teszik – vagyis lesznek olyan dokumentumok, amelyeket többen is olvasnak és többen is szerkesztenek. Ilyenkor nem jó, ha a közös dokumentumból mindenki gépén külön példány van: szükség van egy közös helyre, ahol minden közös dokumentum csak egyszer van tárolva.

Emellett igen költséges lenne mindenki számítógépéhez külön nyomtatót csatlakoztatni – különösen akkor, ha többféle nyomtatási igény van, például kis példányszámú színes és nagy példányszámú fekete-fehér. Ebben az esetben rendszerint kétféle nyomtatóra is szükség van. Olyan technikára is szükség van tehát, amely lehetővé teszi, hogy egy vagy két nyomtatót tízen-tizenötven is használhassanak.

A legtöbb kisirodáról feltételezhetjük, hogy a külső kapcsolatokat elsősorban az interneten keresztül tartják, illetve ugyancsak az interneten ku-

¹ Az amerikai „knowledge worker” kifejezésből.

1. feladat: Kiroda internet-hozzáféréssel

tatnak információ után – tehát a munkatársaknak közös internetkapcsolatra is szükségük van. Régebben volt arra példa, hogy az irodában volt egy „internetes gép”, amelyhez külön oda kellett ülni, ha valaki e-mailezni vagy keresni akart. Ma azonban már bevett dolognak számít, hogy az összes munkatárs számítógépe – egy közös ponton keresztül – kapcsolódik az internethez, és mindenki a saját gépéről érheti el a külvilágot.

A hálózatról és a kiszolgálókról

Ha a dokumentumokat, adatokat, szolgáltatásokat közös helyen tartjuk fenn, ezek eléréséhez hálózatra van szükség. A hálózatban legalább egy kitüntetett számítógép lesz: ez a kiszolgáló. A kiszolgáló tárolja a közös dokumentumokat, futtatja a közösen elérhető programokat, biztosítja a hozzáférést a nyomtatókhoz. Emellett kiszolgálói feladat a közös internet-hozzáférés biztosítása is, bár ezt – különösen kis irodákban – nem a számítógép formájú kiszolgáló, hanem egy céleszköz, az útválasztó biztosítja.

A hálózat haszna: közös dokumentumok, nyomtatók, internet

A számítógépeket általában az erőforrások megosztása és a kommunikáció céljából kapcsoljuk hálózatba. Az alábbiakban röviden összefoglaljuk, mit jelent az erőforrás-megosztás.

A hálózatba kapcsolt számítógépek felhasználói hozzáférhetnek a hálózat más számítógépein tárolt fájlokhoz, használhatják a hozzájuk kapcsolt nyomtatókat, igénybe vehetik a rajtuk futó alkalmazások (például adatbázis-kezelők) szolgáltatásait. Azokat a számítógépeket, amelyek a hálózat más számítógépei számára elérhető erőforrásokat tartalmaznak, *kiszolgálónak* (sokszor *szervernek*) nevezzük; azok a gépek, amelyek felhasználói igénybe veszik a felajánlott erőforrásokat, az *ügyfelek* (más néven *kliensek*).

Az erőforrás-megosztásnak számos haszna van: egy irodában nem kell például valamennyi számítógép mellé nyomtatót venni: ennél sokkal olcsóbb megoldás a számítógépek hálózatba kötése: ekkor csak egy géphez kell nyomtatót csatlakoztatni, és elegendő azt a hálózatban

megosztani. Ha sok felhasználónak szüksége van ugyanarra a fájlra, a hálózat révén elegendő egyetlen számítógépen – a fájlkiszolgálón – tárolni, nem kell valamennyi gép merevlemezére átmásolni, és nem kell attól sem tartani, hogy a különböző módosítások eredményeképp a fájl-nak számos változata keletkezik.

Ha a sokak által igényelt erőforrás egy nagy adatbázis, akkor az adatbázissal együtt az adatbázis-kezelő programot is elegendő egyetlen gépen – az adatbázis-kiszolgálón – futtatni. A felhasználók számítógépei ekkor az adatbázishoz nem közvetlenül, fájlként férnek hozzá: megfelelő program segítségével az adatbázis-kezelő programnak adnak a hálózaton át utasításokat, és ezek eredményét fogadják. Az utasítások bonyolult adatbázisbeli keresésre és adatok módosítására is vonatkozhatnak.

Az olyan alkalmazásokat, amelyekben a nagy teljesítményt igénylő műveleteket a hálózat kitüntetett számítógépei – az alkalmazás-kiszolgálók – végzik, a felhasználók számítógépein pedig csak az alkalmazások kezelőfelülete működik, ügyfél-kiszolgáló (*client/server*) architektúrájú alkalmazásoknak nevezzük. Ha például adott egy raktári és áruforgalmi adatbázis, amely húszezerféle termék számos adatát tartalmazza, és ezek között rövid idő (egy-két másodperc) alatt kell bonyolult gyűjtéseket elvégezni (például megkérdezzük a kenyérfélék fogyasztását az utóbbi fél évben), elegendő, ha a hálózat egyetlen számítógépe tárolja az adatbázist (mert jelentős lemezterületet foglal el), és rendelkezik a keresések gyors elvégzéséhez szükséges számítási teljesítménnyel. A többi gépet csak a parancsok elküldésére, illetve az eredmények fogadására és megjelenítésére kell felkészíteni. Ez egy PC-hálózat kiépítésekor azt jelenti, hogy szükség lesz egyetlen nagyobb teljesítményű kiszolgálóra, a többi számítógép pedig átlagos PC lehet. Ha valamennyi felhasználói számítógépen jelen kellene lennie az adatbázisnak és az adatbázis-kezelő programnak – vagyis nem állna rendelkezésre hálózat –, akkor mindenhol a kiszolgálóhoz hasonló teljesítményű hardverre volna szükség.

De erőforrásként megoszthatók a számítógépek speciális hálózati kapcsolatai is. A hálózat egy számítógépének bérelt vonalú vagy ADSL-internetkapcsolata például szűkös erőforrás: a hálózatot üzemeltető intézmény esetleg nem teheti meg, hogy minden számítógépe számára vásárol internetcsatlakozást. Ekkor az internet-csatlakozással rendelkező számítógép internetkapcsolata is megosztható, így ezen a számítógépen – az átjárón – keresztül a hálózat többi számítógépe is hozzáfér az internethez.

A felhasználói fiókok és a jelszavak

A számítógépen tárolt erőforrások jelentős értéket képviselnek. A „tudásmunkásokat” foglalkoztató irodák – nem pénzben kifejezett – vagyonának jelentős részét a munkatársak számítógépein vagy a fájlkiszolgálón tárolt dokumentumok képviselik. Ezért ezek megőrzése különösen fontos.

A dokumentumok megvédésének fontos eleme, hogy nem engedjük meg illetékteleneknek a dokumentumok elolvasását vagy módosítását. Ezért, mielőtt valaki hozzáférhetne az iroda által használt valamelyik dokumentumhoz, igazolnia kell a jogosultságát. Ez jellemzően úgy történik, hogy meg kell adnia egy nevet és egy jelszót, amelyet a kiszolgáló ellenőriz, és amennyiben rendben találja, lehetővé teszi a hozzáférést.

Ma már az is mindennapos, hogy az egyes számítógépek elindításához is névre vagy jelszóra van szükség. Ez különösen fontos a hordozható számítógépek esetén, mert azokat fizikailag is könnyebb ellopni.

A nevet és a jelszót úgy kell megválasztani, hogy nehezítse a hozzáférést azok számára is, akik betörés céljából próbálják kitalálni a hozzáféréshez szükséges adatokat. Ennek a leghatásosabban úgy vehetjük elejét, hogy csökkentjük a jelszó kitalálásának esélyét. Két szabályt mindenképpen tartsunk be:

1. Válasszunk nehezen kitalálható jelszót! Ne válasszunk olyan értelmes szót jelszónak, amely kötődik hozzánk (saját vagy családtag neve, mindennapi szokás stb.) Ha már értelmes szót választunk, helyezzünk el benne véletlenszerűen számjegyeket, és véletlenszerűen alkalmazzunk kis- és nagybetűket! Egy példa: ha a kutyanék neve Bendegúz, és szeretnénk ezt használni jelszónak, ne adjuk meg pontosan, hanem torzítsuk el, például így: **beN79dEgu7z**. Ne használjunk rövid jelszót sem! A hat-hét karakternél rövidebb jelszavak jelszófeltörő programmal rövid idő alatt kitalálhatók, akkor is, ha nem értelmes szót adtunk meg.
2. Bizonyos időközönként változtassuk meg a jelszót! A Windows-rendszerek beállíthatók úgy, hogy meghatározott rendszerességgel rákényszerítse felhasználóit jelszavuk megváltoztatására.

A felhasználónevet és a jelszót a számítógép úgy tudja ellenőrizni, hogy nyilvántartja a hozzáférésre jogosult felhasználókat. Ezt úgynevezett **biztonsági adatbázisban** teszi. A biztonsági adatbázisban minden felhasználónak van egy fiókja. A felhasználói fiók (*user account*)

tárolja a felhasználó nevét, jelszavát, kapcsolati adatait, és olyan információkat is, amelyek alapján finomabban is szabályozható, hogy a felhasználó mihez férhet hozzá, és mihez nem. A felhasználók például csoportokba szervezhetőek, és minden csoportnak más és más jogokat lehet adni.

A hálózat felügyelete

Hitelesítés és engedélyezés: a hozzáférés szabályozása

A számítógépeken általában részletesen szabályozható, hogy melyik felhasználó mely erőforrásokhoz férhet hozzá. Például nincs mindenkinek szüksége a könyvelési adatokra: a rendszer beállítható, hogy azokat csak a pénzügyi munkatársak láthassák.

A jól védett informatikai rendszer az éppen elégséges jogok elvét alkalmazza, vagyis vigyáz arra, hogy mindenki csak azokhoz az erőforrásokhoz férhessen hozzá, amelyekre a munkájához feltétlenül szüksége van. Ezzel elejét vehetjük annak, hogy védtelenül hagyjunk adatokat, és azokat illetéktelenek akár véletlenül, akár rosszindulatból módosítsák vagy felhasználják.

Az informatikai rendszer az erőforrások védelmét két szinten valósítja meg. Először azt ellenőrzi, hogy a felhasználó jogosult-e egyáltalán hozzáférni magához a rendszerhez. Ehhez rendelkezni kell egy olyan névvel, amely szerepel a biztonsági adatbázisban. Ekkor a rendszernek meg kell győződnie arról, hogy a felhasználó valóban az-e, akinek mondja magát. Ezt a folyamatot hitelesítésnek (authentication) nevezzük. A felhasználónak három eszköze van, amellyel igazolhatja magát:

1. „Amit tudsz”: Titkos jelszó, amelyről feltételezzük, hogy csak a felhasználó ismeri. A legtöbb rendszer általában beéri az ilyen azonosítással: feltételezi, hogy a jelszót csak a bejelentkező felhasználó ismeri. Ez a legkönnyebben áttörhető védelem, mert a jelszóról könnyen tudomást szerezhet más is – akár úgy, hogy a felhasználó óvatlanul elárulja, akár úgy, hogy kommunikációs trükkökkel kicsalják belőle, akár úgy, hogy automatikus eszközzel feltörik.

1. feladat: Kisiroda internet-hozzáféréssel
2. „Amid van”: A felhasználó azonosíthatja magát például intelligens kártyával – de ide tartozik a bankkártya-használat is. Emellett vannak olyan internetes banki rendszerek, amelyek a jelszavas azonosítást SMS-ben is jóváhagyatják. Utóbbi egy előre beállított mobiltelefon-számon történik, amelyhez a felhasználó mobiltelefonjára is szükség van. Utóbbi tehát együtt alkalmazza az „amit tudsz” és az „amid van” módszert.
3. „Ami vagy”: Ez a biometrikus azonosítást – az ujjlenyomat-leolvasást vagy az íriszvizsgálatot – jelenti. Ma már szinte minden új hordozható számítógépen van ujjlenyomat-olvasó, és a rendszer beállítható úgy is, hogy a jelszó megadása mellett az ujjlenyomat leolvasását is igényli. Ez a legbiztosabb hitelesítési módszer, mert olyasmi szükséges a felhasználó azonosításához, amit nem lehet tőle ellopni (nem számítva a balesetet vagy a műtétet).

A hitelesítés után az informatikai rendszer „tudja”, ki a felhasználó. A második lépésben pedig azt kell megvizsgálnia, hogy az illető hozzáférhet-e ahhoz a konkrét erőforráshoz, amelyet igényel. Ez a művelet az engedélyezés (*authorization*). Ezért a rendszer általában minden erőforrás mellett feltünteti, hogy mely felhasználók érhetik el, és milyen műveleteket végezhetnek rajta. Ez utóbbi adat a hozzáférési engedély (*access permission*). A felhasználó tehát akkor érhet el egy erőforrást, ha sikeresen hitelesíti magát a rendszer számára, és rendelkezik engedéllyel az igényelt erőforráshoz.

A címtárszolgáltatás: a felhasználók és erőforrások központi felügyelete

Amikor egy noteszgép a rendszerindításkor nevet és jelszót kér, azt a helyi – tehát a gép saját merevlemezén tárolt – biztonsági adatbázis alapján ellenőrzi. Ez azt is jelenti, hogy az adatbázisban felsorolt felhasználók az adott számítógép helyi erőforrásaihoz férhetnek hozzá – és ezek közül is csak azokhoz, amelyekhez megfelelő hozzáférési engedélyeket kaptak. Az ilyen erőforrások a lemezekben levő mappák és fájlok, a nyomtatók és a kiszolgáló-alkalmazások szolgáltatásai. Az adatbázisban felsorolt fiókok tulajdonosai ugyanakkor a számítógéphez a hálózaton keresztül is kapcsolódhatnak, és az erőforrásokhoz a hálózaton keresztül is hozzáférési engedélyeket szerezhetnek.

Nagyobb hálózatokban a felhasználói fiókok nyilvántartása – és így a hitelesítés – központosítva van. Ez azt jelenti, hogy a felhasználók az egyes számítógépek helyi biztonsági adatbázisa helyett egyetlen közös, központi adatbázisban vannak felsorolva. A központi adatbázisban felsorolt felhasználók – elviekben – a központból felügyelt hálózat minden számítógépén bejelentkezhetnek. Emellett hozzáférhetnek a hálózaton keresztül e számítógépek erőforrásaihoz – természetesen csak azokhoz, amelyekhez rendelkeznek a megfelelő hozzáférési engedéllyel.

Központból felügyelt hálózat létrehozására a legfejlettebb eszköz a címtárszolgáltatás (*directory service*). A címtár olyan adatbázis, amely nyilvántartja a hálózat felhasználóit, számítógépeit és azok erőforrásait – megosztott mappákat, nyomtatókat, kiszolgáló-alkalmazások szolgáltatásait. A címtárszolgáltatás ennek alapján központi helyen végzi a felhasználók hitelesítését, és ezt követően információt ad a felhasználóknak a rendelkezésre álló erőforrásokról, sőt, el is vezeti azokhoz őket. A hálózat felhasználóinak nem kell tudniuk, hogy az egyes hálózati erőforrások konkrétan melyik számítógépen található; elegendő a címtárhoz fordulniuk. A címtár ráadásul strukturált adatbázis, vagyis a hálózat felhasználói és erőforrásai szervezeti egységekbe csoportosíthatók – a hálózatot alkalmazó intézmény felépítésének megfelelően. A Windows kiszolgálóoldali változatai (Windows 2000 Server, Windows Server 2003, Windows Server 2008) tartalmaznak címtárkiszolgálót, melynek neve *Active Directory*. Az *Active Directory*-rendszerben az egyetlen címtáradatbázis által felügyelt hálózat neve *tartomány* (*domain*). A tartomány címtáradatbázisát kezelő számítógépet – kiszolgálót – pedig *tartományvezérlőnek* (*domain controller*) nevezzük. A tartomány többi számítógépe pedig a tartomány tagja (*member*).

A rendszergazda

A magányos felhasználók – a szabadúszó tudásmunkások – és a kisirodák gyakran magukra maradnak az informatikai rendszer üzemeltetésében. Ez azt jelenti, hogy az erőforrás-megosztás kialakítását, a kiszolgáló és az internet-hozzáférés telepítését önerőből, autodidakta módon tanulják meg. Ilyenkor általában elmaradnak a megfelelő biztonsági beállítások; a rendszer, a hálózat vagy túlságosan zárva, vagy – ami gyakoribb – túlságosan nyitva van.

1. feladat: Kisiroda internet-hozzáféréssel

Olyan irodában, ahol többen dolgoznak együtt, és a közös erőforrásokat kiszolgáló segítségével veszik igénybe, mindenképpen szükség van valakire, aki

- megtervezi a hálózatot, a kiszolgálót és az adatvédelmi beállításokat,
- telepíti a rendszert, és beállítja az erőforrások megosztását,
- segít fenntartani a rendszert: elvégzi vagy beállítja a biztonsági mentéseket, és elhárítja a hibákat.

Az a személy, aki a fenti feladatokat végzi, a **r e n d s z e r g a z d a**. Kisirodában rendszerint nincs szükség főállású rendszergazdára; vannak olyan rendszergazdák, illetve cégek, akik (amelyek) több iroda informatikai rendszerét üzemeltetik, többnyire óradíj ellenében.

A „rendszergazda” szónak van még egy jelentése. Említettük, hogy a számítógépek és a kiszolgálók biztonsági adatbázisában vagy a címtár-adatbázisban fel vannak sorolva azok a felhasználók, akik hozzáférhetnek a rendszer erőforrásaihoz. Írtuk azt is, hogy ezek a felhasználók különböző jogokkal rendelkeznek.

A felhasználói fiókok között vannak olyanok, amelyek úgynevezett rendszergazda-jogokat kaptak. Aki ilyen felhasználói fiók nevével és jelszavával jelentkezik be, a rendszer minden erőforrását elérheti, és azokkal minden lehetséges műveletet elvégezhet.

Vannak a rendszerben olyan tevékenységek, amelyekre csak rendszergazda-jogok birtokában van lehetőség. Ilyen például az alkalmazások telepítése, egyes rendszerszintű jogosultságok vagy beállítások módosítása.

Biztonsági szempontból nagyon fontos, hogy az iroda informatikai rendszerében csak azok rendelkezzenek rendszergazda-jogokkal, akiknek erre feltétlenül szükségük van. Ha tehát az ügyvezető igazgató nem végez informatikai karbantartási feladatokat, kimondottan káros, ha rendszergazda-jogokat kér vagy kap. Attól ugyanis nem lesz valakinek több ellenőrzése az erőforrások fölött, ha bármit csinálhat velük, ám kellő szakértelem híján nem ismeri a lehetőségeket és nem érti a beállításokat. Kisirodában rendszerint két személynek célszerű rendszergazda-jogokat adni: az egyik maga a rendszergazda – aki csak időnként dolgozik a rendszerrel –, a másik pedig egy belső felelős, akit a rendszergazda betanít egyes alapvető karbantartási műveletek (például a biztonsági mentés) elvégzésére.

A hálózat

Helyi hálózat, nagy távolságú hálózat, internet

Ha egy iroda vagy egyetlen épület számítógépeit kapcsoljuk össze, helyi hálózat (*local area network, LAN*) jön létre. Több, esetleg egymástól távol levő hálózat vagy számítógép összekapcsolásakor már nagy távolságú hálózatról (*wide area network, WAN*) beszélünk. A hálózatban részt vevő számítógépek – szakkifejezéssel: állomások (*host*) – közötti távolság alapvetően meghatározza a számítógépek közötti kapcsolat technológiáját.

Külön kategóriának tekinthetjük a mindössze néhány (legfeljebb tízhatsz) gépet összekapcsoló, kitüntetett kiszolgálót általában nem tartalmazó helyi hálózatot. Ilyen hálózatot sokan már otthon is kiépítenek: ha több számítógépük van, valamilyen módon összekapcsolják azokat. Azonban sok kis iroda is épít hasonló hálózatot. Az ilyen hálózatokat kisirodai hálózatnak (*small office network*) nevezik.

A helyi hálózatok fizikai felépítése általában egynemű, a legegyszerűbb esetekben a hálózatnak egyetlen gerincvonala van, és minden állomás ahhoz csatlakozik. Az egyneműség különben azt jelenti, hogy az állomások összekötésére a hálózatban mindenhol ugyanolyan szabványú átviteli közeg – többnyire kábelezés vagy rádiócsatorna – szolgál.

A nagy távolságú hálózatok ezzel szemben rendkívül vegyesek: ezek a legkülönbözőbb felépítésű és szabványú hálózatokat kötik össze egyetlen, nagyobb hálózattá. A nagy távolságú hálózatok legegyszerűbb esete, amikor adott egy helyi hálózat, amelynek egyik számítógépéhez telefonvonalon csatlakozik egy távol levő felhasználó számítógépe, s ily módon hozzáfér a helyi hálózat erőforrásaihoz. A legbonyolultabb nagy távolságú hálózat az internet, amely több millió állomást tartalmaz: ha az interneten egy állomás üzenetet küld egy másiknak, az üzenet számos, rendkívül különböző hálózatszakaszon halad át: helyi hálózatokon, a nyilvános telefonhálózaton, bérelt vonalakon, mikrohullámú csatornákon stb.

Ennek a könyvnek nem tárgya a hálózatok fizikai felépítése. Minden, itt leírt művelethez feltételezzük, hogy a hálózat – fizikai mivoltában – ki van építve. Azt viszont tudnia kell az Olvasónak, hogy nem csak a kiterjedés, hanem a minőség és a használat jellege szempontjából is lényeges különbség van a helyi és a nagy távolságú hálózatok között: az előbbie-

ben – ma még – az erőforrás-megosztás dominál, addig az utóbbiakban – különösen az interneten – a kommunikáció: az erőforrásokhoz való hozzáférés az internet fölött egyoldalú, általában webdokumentumok letöltését – olvasását – jelenti. A technikai kivitelezés különbségeiből is következik, hogy a helyi hálózaton belül két állomás között lényegesen gyorsabb és megbízhatóbb adatátvitel lehetséges, mint a nagy távolságú hálózatokban. Az utóbbi korlátait a hálózatban megjelenő nyilvános szakaszok, illetve a távolsági vonalak kiépítésének magas költségei okozzák. A távolsági vonalak minőségének javulásával és költségeik csökkenésével azonban a különbségek egyre kisebbek.

A hálózat sávszélessége és megbízhatósága

Két állomás között az adatátvitel minőségét a kapcsolat sebessége és megbízhatósága határozza meg. Mivel a hálózati kapcsolat alapja az elektromágneses (vagy optikai) jelátvitel, a sebesség közvetlenül kapcsolatba hozható a sávszélességgel (*bandwidth*). Az átviteli sebességet és a sávszélességet ezért gyakran felcserélik, holott a sávszélesség az átviteli sebesség lehetősége csupán. Maga a tényleges átviteli sebesség attól is függ, hogy milyen minőségű a kapcsolat; hibák esetén ugyanis sok adatot újra kell küldeni, ami pedig jelentősen csökkenti a felhasználó – a külső megfigyelő – számára látható átviteli sebességet. A tényleges átviteli sebesség így sokkal kisebb is lehet, mint amekkorát a vonal sávszélessége lehetővé tesz.

A sávszélességet – az adott vonalon elvileg lehetséges legnagyobb átviteli sebességet – az egységnyi idő alatt továbbítható adatok mennyiségével adjuk meg. Az egységnyi idő a másodperc (*second*; *s*), az adatok legkisebb átvihető egysége pedig a *bit* – egyetlen kettes számrendszerbeli számjegy. Kellően nagy sávszélesség akár több millió, sőt több milliárd bit továbbítását is lehetővé teszi egyetlen másodperc alatt, így beszélünk kilobitról (*kbit*; 1024 bit) megabitról (*Mbit*; 1024 kbit) és gigabitról (*Gbit*; 1024 Mbit) is. A sávszélességet – és a tényleges adatátviteli sebességet – így *bit/s*-ban, *kbit/s*-ban vagy *Mbit/s*-ban adjuk meg. 1 *bit/s* egyetlen bit átvitelét jelenti egy másodperc alatt; 1 *kbit/s* esetén 1024, 1 *Mbit/s* esetén 1024·1024 bit jut el a partnerhez egyetlen másodperc alatt.

Az ismertebb hálózattípusok jellemző sávszélességei a következők:

<i>Hálózattípus</i>	<i>Sávszélesség</i>
Analóg telefonvonal	33,6 - 56 kbit/s
ISDN-vonal	64 kbit/s, több vonal nyalábolása esetén ennek többszörösei
ADSL, ADSL 2	Letöltési sebesség: 1 Mbit/s - 18 Mbit/s, jellemző feltöltési sebességek: 128 kbit/s - 1 Mbit/s
Kábeltelevízió-hálózat	1 Mbit/s - 10 Mbit/s (jellemző sebességek)
Ethernet (helyi hálózat)	100 Mbit/s, 1 Gbit/s, 10 Gbit/s
ATM, FDDI	144 - 622 Mbit/s

A kommunikáló állomások között ténylegesen mért adatátviteli sebesség általában nem éri el a sávszélességet. Az alkalmazott hálózati technológia ugyanis megszabja, hogy a sávszélesség milyen mértékben használható ki hatékonyan. Így például a legelterjedtebb helyi hálózati technológiában, a 100 Mbit/s sávszélességű Ethernetben jellemzően kb. 7-8 Mbytenyi adat továbbítható egy másodperc alatt, holott a 100 Mbit/s sávszélesség elvileg 12,5 Mbyte továbbítását is lehetővé tenné (1 byte = 8 bit).

Amikor pedig az adattovábbítás megbízhatóságáról beszélünk, három szempontot vizsgálunk:

1. A továbbított adatok helyessége: Pontosan azok az adatok (adatbitek) érkeznek-e meg a címzetthez, amelyeket a forrás elküldött? Ha esetleg nem, ez ellen védekezni kell: az adatokat hibajavító információval ki kell egészíteni, hogy a hibásan átvitt bitek javíthatók legyenek.
2. Az adatok sorrendje: Az üzenetek részei megfelelő sorrendben érkeznek-e meg? Ha esetleg nem, a sorrendet a csomagok sorszámozásával ellenőrizni kell, és a címzettnél helyre kell állítani.
3. Teljesség: Hiánytalanul megérkezik-e minden? Ha esetleg nem, azonosítani kell a kimaradt részt, és azt a forrásnak újra kell küldenie. Annak megállapítására, hogy egy adatcsomag megérkezett-e, a címzett nyugtát küld a forrásnak.

Vegyük észre, hogy sem a kiegészítő hibajavító információ, sem a csomagsorszám, sem a nyugta, sem pedig az újraküldött csomag nem része a „hasznos” - a felhasználó számára látható - adatfolyamnak. Ezek is felémésztik a sávszélesség egy részét, ezért ha hibákra kell számítani - márpedig elektromágneses jeltovábbítás esetén kell -, eleve nem használható hasznos adattovábbításra a teljes sávszélesség.

Az átvitelben részt vevő vonalszakaszok számának, illetve hosszának növekedésével ugrásszerűen nő a hibák valószínűsége: a vonal nagyobb zajnak van kitéve. Ezért a helyi hálózati kapcsolatok sáv szélessége és megbízhatósága is sokkal nagyobb, mint a nagy távolságú kapcsolatoké. A hálózaton keresztül kommunikáló programoknak pedig minderre fel kell készülniük: másképpen kell kommunikálniuk a helyi hálózatban, és másképpen nagy távolságú vonalakon.

A protokollok és a hálózatban levő gépek megcímzése

Amikor a hálózat szolgáltatásait használjuk, természetesnek vesszük, hogy meg tudjuk nyitni a kiszolgálón tárolt dokumentumainkat, nyomtatni tudunk a kollégánk gépéhez kötött nyomtatón, tudunk elektronikus levelet küldeni, és így tovább. Kézenfekvőnek tekintjük, hogy a számítógép könyvtárait, nyomtatóit meg tudjuk osztani, ahhoz pedig, hogy más számítógépek megosztott könyvtáraiból fájlokat olvassunk, elegendő például a szövegszerkesztő tallózóablakát oda irányítani vagy a `\\számítógép\mappa` formában megadni a hálózaton érvényes elérési utat.

Mindezek a hálózati szolgáltatások nem állnak rendelkezésre pusztán attól, hogy a számítógépekben hálózati csatolókárttyák vannak, azokon keresztül pedig kábellel össze vannak kötve a számítógépek. Ha az állomások között létezik is az elektromos kapcsolat, az adatátvitelhez komoly párbeszédre van szükség a két állomás (pontosabban a két állomáson futó programok) között. Ennek a párbeszédnek rendkívül sok eleme, szintje van; s ezek mindegyikére szükség van ahhoz, hogy a kollégánk számítógépére eljusson az a dokumentum, amelyet ki akarunk nyomtatni.

A hálózati kommunikáció javarészt szabványos elemekből áll; szükségtelen tehát az alkalmazásoktól elvárni, hogy az adattovábbításhoz szükséges teljes párbeszédet maguk bonyolítsák le. A szövegszerkesztő, amelyből nyomtatunk, nem is képes ilyen párbeszédre, csak annyira, hogy a hálózatban megnevezze a kívánt fájlt vagy nyomtatót. Minden egyebet elvégez helyette az operációs rendszer, amelynek abbéli feladata, hogy erőforrásokat bocsásson a felhasználók és az általuk elindított programok rendelkezésére, kiterjed a hálózati – más számítógépeken található – erőforrások biztosítására is. Az operációs rendszernek tartalmaznia kell a hálózati kommunikációhoz szükséges valamennyi szoftverelemet – a hálózati csatolókárttya illesztőprogramjától azokig a magas szintű modu-

lokig, amelyek a \\kiszolgáló\könyvtár vagy a <http://kiszolgáló/mappa/fájl> stb. formájú elérési utak alapján meg tudják keresni a hálózatban a felhasználó által kívánt állomást.

Az operációs rendszerben mindenképpen vannak olyan modulok, amelyek

- működtetik a megbízható adattovábbítást két, azonos helyi hálózatba eső állomás között;
- név vagy cím alapján megtalálják a címzett állomásokat (számítógépeket);
- működtetik a megbízható adattovábbítást bármely két állomás között, bárhol is legyenek a hálózatban.

Ezek a modulok sajátos szabályok szerint működnek. A szabályok arra vonatkoznak, hogy két állomásnak milyen módon kell kommunikálnia egymással. A szabályokat és a modulokat is `protokollnak` (protocol) nevezik. A protokoll eredetileg a szabályok neve, ám a megvalósított rendszerekben alkalmazzák az őket működtető programrészekre is.

A hálózatba kötött számítógépek rendszere olyan, mint a posta: minden számítógépnek van egy címe. Ez a cím jellemzően egy bonyolult szerkezetű szám. A felhasználók azonban nem ezekkel a számokkal, hanem könnyen megjegyezhető nevekkel címezik meg a gépeket. Ezért a hálózatban működik olyan mechanizmus, amely a név alapján először megkeresi a címzett állomás (számítógép) számmal kifejezett címét. Ez a mechanizmus a *névfeloldás* (*name resolution*). Az interneten – és olykor a helyi hálózatban – vannak olyan kiszolgálók, amelyekhez névfeloldási kérésekkel lehet fordulni. Az ilyen kiszolgálók – a *név-kiszolgálók* (*name server*) –, amikor megkapják egy számítógép nevét, a számmal kifejezett címet küldik vissza.

A vezeték nélküli hálózat

A számítógépek összekapcsolásának legolcsóbb módja a vezeték nélküli hálózat. Ehhez be kell szerezni egy úgynevezett vezeték nélküli hozzáférési pontot (*wireless access point*, WAP). A hozzáférési pontnak kell adni egy nevet. Azok a számítógépek tartoznak egy vezeték nélküli hálózatba, amelyek azonos vezeték nélküli hozzáférési ponthoz kapcsolódnak.

1. feladat: Kisiroda internet-hozzáféréssel

A vezeték nélküli hálózatnak azonban vannak hátrányai a vezetékes hálózathoz képest. A hálózat kiterjedése általában nem probléma; a vezeték nélküli hálózat hatótávolsága 10-50 méter. Azonban a hálózati technológia kiválasztásakor oda kell figyelni a következőkre:

1. A vezeték nélküli hálózat sávszélessége kisebb. Általában 54 Mbit/s sávszélességet ígér, ez azonban a gyakorlatban sohasem több 10-20 Mbit/s-nél – miközben a vezetékes hálózatokkal akár 1 Gbit/s sávszélességet is el lehet érni (olcsó eszközökkel is). Nagy mennyiségű adat továbbítására ezért a vezeték nélküli hálózatok alkalmasabbak.
2. A vezeték nélküli hálózat forgalma „kihallatszik”: alkalmas eszközökkel akár az utcán el tudják olvasni, milyen adatok utaznak a hálózatban. Ezért a vezeték nélküli hálózatban mindig oda kell figyelni a titkosításra, ami nem mindig egyszerű feladat.
3. A vezeték nélküli hálózat nem mindig használható olyan helyeken, ahol sok vezeték nélküli hálózat működik egy területen. A hozzáférési pont beállítható egy meghatározott csatornára, ám rendszerint csak 11 csatorna közül lehet választani, ráadásul a hálózatok működtetői erre általában nem figyelnek oda. Az azonos csatornára állított hálózatok zavarhatják egymást, ami csatlakozási problémákat okozhat: a legjobb esetben is jelentősen megnő a számítógépek csatlakozásához szükséges idő.

Hozzáférés az internethez: az útválasztó

Az internet-hozzáférés szűkös erőforrás, ezért a kisiroda jellemzően csak egy internetkapcsolattal rendelkezik. Ez azt jelenti, hogy nem az egyes munkatársak gépeit, hanem az egész hálózatot kell az internethez kapcsolni. A hálózatban ezért lesz egy olyan berendezés, amely két hálózat-hoz kapcsolódik: az egyik a belső (helyi) hálózat, a másik pedig az internet, pontosabban az internetszolgáltató hálózata. Kifelé – az internet számára – a kisiroda hálózata egyetlen állomásnak látszik: a hálózatot ez a bizonyos berendezés képviseli.

Ez a berendezés az *útválasztó (router)* vagy *átjáró (gateway)*. Az útválasztó gondoskodik arról, hogy a belső (helyi) hálózat gépeiről indított kommunikáció eljusson a hálózaton kívüli címzethez, illetve a külső hálózatból (az internetről) érkező válasz eljusson a megfelelő belső állomáshoz (számítógéphez).

Az útválasztó szerepét betöltheti egy közönséges számítógép is, amelyben két hálózati csatolókártya van – egy a belső, egy a külső hálózat irányába –, de sok esetben külön berendezést alkalmaznak, amely csak útválasztóként tud működni, ám olcsóbb, mint egy külön számítógép.

Az internet-hozzáférés biztonsági megfontolásai

Az internet számítógépek millióit összekapcsoló, mindenki számára hozzáférhető rendszer. Ennek az a hátránya, hogy a rosszindulatú felhasználása előtt is szabad az út. Ha egy számítógépet az internetre csatlakoztatunk, biztosak lehetünk benne, hogy percekben belül éri valamilyen támadás, ami arra irányul, hogy adatokat olvassanak le róla, vagy átvegyék fölötte az irányítást. Ezért az internetre kapcsolt számítógépeket vagy helyi hálózatokat védeni kell, és a megfelelő védelmet még a kapcsolat létrehozása előtt üzembe kell állítani.

A védelem eszköze a tűzfal (*firewall*). Ez olyan program, amely folyamatosan figyeli a hálózatból induló és a felé irányuló hálózati forgalmat. Olyan szolgáltatásokat nyújt, amelyek segítségével észlelhetők a rosszindulatú kapcsolódási kísérletek, a weboldalakban vagy a levelekben elrejtett vírusok és trójai falovak, és meghatározott forgalomtípusok ki is zárhatók a kommunikációból.

Lássuk, milyen szolgáltatásokat nyújtanak az egyes tűzfalak:

- **Betörés-érzékelés (*intrusion detection*):** Van néhány jellemző művelet, amelyeket a támadók megpróbálnak elvégezni a célrendszeren. A betörés-érzékelő tűzfalak a hálózati forgalomban megpróbálják felismerni ezeket a műveleteket, és jelezni a felhasználónak, illetve blokkolni a támadótól érkező forgalmat.
- **Csomagszűrés (*packet filtering*):** Annak szabályozása, hogy a hálózat milyen típusú csomagokat fogad el, illetve a rajta futó programok milyen fajta csomagokat küldhetnek.
- Sok esetben szabályozható az is, hogy mely címekről (mely számítógépekről) fogadjuk, illetve utasítjuk el a forgalmat. Egyes tűzfalakban pedig a csomagok tartalma is megszabható, bár ez a személyi tűzfalakban nem jellemző. Azonban, ha egy tűzfal víruskereső programot tartalmaz, már egyfajta – jól irányított – tartalomszűrésnek tekinthető.

1. feladat: Kisiroda internet-hozzáféréssel

- Alkalmazások szűrése: Számos rendszerben meghatározható, hogy az interneten keresztül mely programok kommunikálhatnak. Ha ez szabályozva van, a támadó által telepített trójai faló – amelynek a felhasználó számítógépét kellene vezérelnie – többnyire nem működik majd, hiszen számára nincs engedélyezve a hálózat használata.

A kisirodai hálózatot rendszerint olyan – az útválasztóval egybeépített – tűzfallal védik, amely alapértelmezés szerint minden kívülről irányuló kapcsolati kérést megakadályoz, és csak a hálózat belsejéből küldött kérésekre adott válaszokat engedi be a hálózatba.

A hibák megelőzése és elhárítása

Az adatok mindig veszélyben vannak

Közhely, hogy ami elromolhat, az el is romlik. Írtuk, hogy a tudásmunkások által létrehozott dokumentumok olykor a cég vagyonának jelentős részét alkotják, ezért minden áron meg kell őket védeni. A dokumentumokkal – az informatikai rendszerrel – kétféle baj történhet:

Az informatikai rendszer elérhetetlenné válhat. Ez azt jelenti, hogy a dokumentumokhoz vagy a rendszer szolgáltatásaihoz nem tudunk hozzáférni – gyakran éppen akkor, amikor a legnagyobb szükségünk van rá. Ilyenkor, bár az adatok nem vesznek el, az okozhat nagy kárt, hogy nem tudunk a megfelelő időben (például a határidő előtt félórával) hozzájuk férni.

Az informatikai rendszer meghibásodhat, az adatok megsérülhetnek vagy elveszhetnek. Ebben az esetben a kár állandó: a sérült vagy megsemmisült dokumentumokban fekvő szellemi tulajdont újra létre kell hozni.

Ezért az informatikai rendszerek védelme azt jelenti, hogy fenntartjuk a rendszer rendelkezésre állását (*availability*) és megóvjuk az adatok épségét (*data integrity*).

A hálózat és a kiszolgáló karbantartása

A rendelkezésre állást azzal tudjuk biztosítani, hogy felkészülünk az esetleges rendkívüli eseményekre (meghibásodásokra). Ha pedig bekövetke-

zik a rendkívüli esemény, megfelelő ismeretekkel és stratégiával kell rendelkezni arra, hogyan derítsük ki a hiba okát, és hogyan állítsuk vissza mihamarabb a rendszer működését.

Az áramszünetek ellen például szünetmentes áramforrás alkalmazásával védekezhetünk. A rendszerindításhoz használatos merevlemez meghibásodása ellen pedig két merevlemez alkalmazásával és a rendszerterületek tükrözésével.

A rendkívüli események kezelése nemcsak technikai eszközök alkalmazását jelenti. Amikor a rendszer meghibásodik, a hibát elhárítani képes személynek elérhetőnek kell lennie, illetve megfelelő időben értesülnie kell róla. A kiszolgáló elérhetőségét, üzemképességét például lehet figyelni egy másik rendszerből, és amikor valami nem működik megfelelően, a rendszergazda automatikusan értesülhet róla.

Vannak olyan események, amelyek előre jelzik, hogy a rendszer hamarosan meghibásodik vagy elérhetetlenné válik. Folyamatosan működő számítógépek esetén erre utal, ha a rendelkezésre álló szabad memória vagy merevlemez-terület folyamatosan csökken, vagy a rendszer eseménynaplójában lemezhibákra utaló bejegyzések jelennek meg.

A biztonsági mentés és az adatok épségének védelme

Amikor olyan meghibásodás következik be, amelyben az adatok is megsérülnek, a hiba elhárításának legfontosabb eleme az adatok helyreállítása. Biztosak lehetünk abban, hogy az informatikai rendszer életében legalább egyszer bekövetkezik ilyesmi, ezért az adatvesztésre előre fel kell készülni.

Ezért a védekezés legfontosabb eleme a biztonsági másolatok készítése. Az irodai hálózat számítógépein tárolt adatokról rendszeresen másolatot kell készíteni. Ha a közös dokumentumok valamennyien egy kiszolgálón vannak, elsősorban a kiszolgáló biztonsági mentéséről kell gondoskodni.

A biztonsági mentésnek mindenképpen külső adathordozóra kell készülnie. A rendszeresség pedig azt jelenti, hogy a másolatoknak naprakésznek kell lenniük, vagyis - az iroda tevékenységétől függően - legfeljebb egy-két napnyi munka elvesztését lehet eltérni. Ez azt jelenti, hogy az adatokról - legalább azokról, amelyek időközben megváltoztak - na-

1. feladat: Kiroda internet-hozzáféréssel

ponta-kétnaponta kell másolatot készíteni. Ezt a folyamatot részben automatizálni is lehet.

A biztonsági másolatokat nem szabad az irodában tárolni. Ez azért fontos, mert ha az irodában fizikai kár – betörés, beázás, tűz stb. – történik, a biztonsági másolat nem pusztul együtt a kiszolgáló merevlemezével.

Az adatok épségét más módon is védeni kell. A számítógépek merevlemeze általában hirtelen hibásodik meg (bár ennek lehetnek előjelei). Ilyenkor sokat segít, ha a merevlemez tükrözve van, vagyis a számítógép két merevlemez tartalmaz, és az új adatokat automatikusan mindkettőre felírja.