Nemzeti Információs Infrastruktúra Fejlesztési Program

Információs Füzetek 11.8.

DRAVECZ TIBOR · PÁRKÁNYI BALÁZS

# HOGYAN VÉDJÜK HÁLÓZATRA KÖTÖTT SZÁMÍTÓGÉPES RENDSZEREINKET?

Budapest

1996

Dravecz Tibor

Párkányi Balázs

# Hogyan védjük hálózatra kötött számítógépes rendszereinket?

**NIIF Információs Füzetek II. 8.**

**© Dravecz Tibor (dravecz@fa.gau.hu)**

**© Párkányi Balázs (balazs@fa.gau.hu)**



ISBN 963 02 9941 0

ISSN 1219-5472

Kiadja a Nemzeti Információs Infrastruktúra Fejlesztési Program Koordinációs Iroda

NIIFKI vezetője: Nagy Miklós

A kiadásban közreműködött: Kornétás Kiadó

Ügyvezető igazgató: Pusztay Sándor

Műszaki szerkesztő: Gáspár Imre

Nyomta: Komáromi Nyomda és Kiadó Kft. — 96-875

Felelős vezető: Kovács Jánosné ügyvezető igazgató

Dravecz Tibor

Párkányi Balázs

# Hogyan védjük hálózatra kötött számítógépes rendszereinket?

II. 8.



N.I.I.F.

Budapest, 1996

**Tartalom**

Tartalom

# Bevezetés

A számítógépek és a számítógépes adatok védelme egyre növekvő jelentőséggel bír, ennek megfelelően egyre nagyobb érdeklődés mutatkozik a számítógép-biztonság iránt. A védelem jelentősége lényegesen megnőtt a hálózatok megjelenésével, a védekezés összetettebbé és bonyolultabbá vált, s a felhasználóknak ugyanakkor eddig nem ismert veszélyforrásokkal kell szembenézniük. Tévhitek terjedtek el mind a veszélyforrásokról, mind a védekezési módokról.

E füzetet az akadémiai szférában (egyetem, iskola, közintézmény) tevékenykedő számítógép-felhasználóknak szánjuk. Nem foglalkozunk titkos vagy üzleti adatok védelmével, bár utalásokat teszünk ilyen irányba is. Noha az akadémiai szférában egyes esetektől eltekintve alacsonyak a biztonsági követelmények, az oktatásnak ezen túl kell mutatnia, nem lehet általános példa a laza biztonsági menedzsment. Szigorúan platform- és alkalmazás-független módon igyekszünk mindent tárgyalni, mindemellett figyelembe véve az Internet felhasználók érdeklődését. Azonban **nem Internet biztonsági könyvet írtunk**, abban a meggyőződésben, hogy az Internet felhasználás biztonsági kérdéseit nem érdemes szétválasztani az általános számítógép-biztonsági kérdésektől. Megpróbáltunk az általános kérdésekre, elvekre koncentrálni, lehetőleg azon kérdésköröket tárgyalni, melyek nem egyik napról a másikra változnak. Az aktuális információk forrásának ott van maga az Internet, ill. a World-Wide Web.

Ezen írást nem professzionális felhasználóknak szántuk, hanem azoknak, akik csak használni akarnak vagy kényszerülnek (hálózatba kötött) számítógépeket.

Azt tanácsoljuk, hogy füzetünket bevezető olvasmánynak tekintsék, s tanulmányozzák a hely, alkalmazás és operációs rendszer specifikus kérdéseket is. (**Megfelelő védelem csak saját rendszerünk megfelelő ismeretében lehetséges.**) Elengedhetetlen, hogy a felhasználók tisztában legyenek az általuk használt rendszerek, szoftverek alapjainak (biztonsági alapjainak) ismeretével. Tanulmányozni kell a használt berendezések, szoftverek stb. leírásait, meg kell ismerni a helyi működési szabályokat, rendet.

Rögtön itt a bevezetőben nyomatékosan felhívjuk a figyelmet arra, hogy a biztonság alapja a jó **menedzsment**, a megbízható és kellően **integrált hardver és szoftver**, a **szakképzettség** és a **kulturált használat**.

A füzet nyilvánvaló hiányossága, hogy rendszerfüggetlen módon próbálja tárgyalni a számítógép-biztonsági kérdéseket. Minden bizonnyal lehetetlen lenne egy füzetbe belesűríteni Unix, NT, NetWare, VMS rendszerek akár csak minimális biztonsági specialitásait, nem beszélve az adatbáziskezelők, DOS/Windows alatti Internet szoftverek, helyi levelezőrendszerek, modemkonfigurálás stb. ismertetéséről.

Természetesen a felhasználónak nem elég az általános alapelveket tudnia, ismernie kell az általa használt rendszerek, programok biztonsági alapjait is. Ez túlmegy tárgykörünkön, azonban hisszük, hogy az olvasó az általános biztonsági ismeretek birtokában könnyebben sajátítja el az adott rendszerek, alkalmazások biztonsági kérdéseit, jobban felfigyel a problémákra, tennivalókra. Hisszük ezt annál is inkább, mivel tapasztalatunk azt mutatja, hogy a felmerülő problémák, hibák, biztonsági események többsége nagy mértékben rendszerfüggetlen.

A füzethez felhasználtunk számos - az Integrity Informatikai Kft. által készített - nem publikált írást és tájékoztató anyagot. A közreműködőknek, elsősorban Kollár Ágnesnek és Lemle Gézának ezúton mondunk köszönetet.

# 1. Alapfogalmak

## Számítógép-biztonság

**Számítógép-biztonság** *(computer security)* alatt szűkebb értelemben az adatok illetéktelenek hozzáférésétől való védelmét, elsősorban a titkosságot *(secrecy, confidentiality)* értik.

Tágabb értelemben az alábbi hármast értjük rajta:

- **titkosság** és **hozzáférési kontroll** *(access control)*;
- **integritás** (sértetlenség - *integrity*, pontosság - *accuracy*, hitelesség - *authenticity*);
- **elérhetőség** *(availability)*;

és gyakran még egy negyedik szempontot:

- **megbízhatóság** *(reliability)*, melyen a hardver, a szoftver s a szolgáltatások üzembiztonságát értjük, azaz, hogy rendszerünk azt és úgy végzi-e, amint az elvárható/elvárt, elfogadható karbantartási igény és meghibásodásszám mellett. Ez több, mint a rendszer elérhetősége.

A **megbízhatóság**on egy más fogalmat is értünk: azt, hogy mennyire lehetünk biztosak rendszerünk megbízható működésében, védettségében - mennyire tesztelt, igazolt annak védelme *(trustiness)*.

A fenti fogalmakba beleértjük, hogy megfelelő kontrollal rendelkezünk rendszerünk felett, hitelesen nyomon tudjuk követni a biztonsági eseményeket.

Előtérbe került - bár közvetlenül nem tárgya a fentieknek - az ember és a környezet védelme is. A nem megfelelő környezet természetesen veszélyt jelent a számítógépes rendszerekre és a számítógépes munkavégzésre nézve is, de ennél is fontosabb az ember és környezete védelme.

## Mit védünk? Sebezhetőség

Nagyon fontos tudnunk: mit és miért védjünk/védünk, mennyit ér meg a védelem? Ehhez a **sebezhetőség**ünket *(vulnerability)*, a **kockázat**ot *(risk)* és a védekezés módját, a választható **óvintézkedés**eket *(counter-measures)* kell ismernünk.

A sebezhetőség főbb típusai:

- fizikai sebezhetőség;
- hardver, szoftver, média (adathordozó) sebezhetőség;
- kommunikációs sebezhetőség;
- humán sebezhetőség.

A megfelelő óvintézkedésekhez tudnunk kell a támadási lehetőségekről, a **veszélyforrás**okról (*threats*). A veszélyforrások és a sebezhetőség egyes típusai között egyszerűen leírható kapcsolatok vannak. A főbb veszélyforrások a következők:

- fizikai veszélyek;
- gondatlan (nem szándékos) károkozás;
- szándékos támadás (alkalmi rosszakarók, számítógép-betörők - *crackerek, hackerek*);
- programozott kórokozók (közismert példa a számítógép-vírus);
- program és konfigurációs hibák, hardver hibák;
- házon belüli és házon kívüli támadók (*insiders* és *outsiders*).

A megfelelő védelem az arányos védelem, ahol a védendő érték, a potenciális veszély, a védekezés által okozott kellemetlenség ésszerű arányban áll a védelemre fordított költségekkel és erőfeszítésekkel. Általában az adatok jelentik a legnagyobb értéket, egyes helyeken pedig a folyamatos üzem elengedhetetlen. Az akadémiai szférában és az otthoni felhasználóknál az adatok értéke relatíve kisebb, az üzembiztonság szintén csekélyebb jelentőségű, ennek megfelelő a felelősség is. Amíg az adatvesztés egy cég életébe kerülhet, itt csak múló fájdalmat jelent - azonban ez lehet igen kellemetlen is, akár évek munkája is veszendőbe mehet. A privát szférával szemben azonban a védekezés itt sem könnyebb. Nyílt, eleve nem biztonságos környezetben kell megfelelő védelmet biztosítani. (Természetesen nem az erőforrások elzárásával fokozandó a biztonság!) Oktatási intézményekben pedig inkább jó, mint rossz példát kellene mutatni.

## 2. Biztonsági menedzsment és adminisztráció

**A megfelelő menedzsment a védelem alapja.** Ez igaz mind az egyfelhasználós környezetre (otthoni felhasználóra), mind a többfelhasználós (intézményi, vállalati) környezetre, de az utóbbi sokkal összetettebb, a vezetőség által elrendelt szabályzatokon és a kialakult szokásokon nyugszik. Nélkülözhetetlen, hogy írott szabályok rögzítsék az alapvető illetékességi, felelősségi, hierarchikus viszonyokat. Szintén nélkülözhetetlen, hogy világosan és pontosan megfogalmazott és kihirdetett felhasználási politika, üzemeltetési szabályzatok legyenek.

A menedzsment része a biztonsági menedzsment, a felhasználási politika részben magában foglalja a biztonsági politikát. Követelmény, hogy a biztonsági politika szintén írásos alapon nyugodjon, nyílt legyen, azaz nyilvánosan hozzáférhető, s ne tartalmazzon bizalmas elemeket (a szerzők véleménye szerint). Természetesen a biztonsági politikát be kell tartani és tartatni. Emiatt fontos, hogy az ésszerűség határai között legyen csak szigorú (tartalmazzon kötelező és ajánlott elemeket).

A biztonsági politika legfontosabb elemei, a legfontosabb kívánalmak:

- világos, pontos, körülhatárolt, előre meg- és kihirdetett, mindent lefedő legyen;
- jelölje meg az illetékességi viszonyokat, határozza meg a felelősségeket és a felelősöket, a felelős személyek valóban felelősök legyenek;
- hálózatok, fontosabb berendezések (routerek, domain név szolgáltatás, hálózatmenedzsment eszközök és hasonlóak) és nagyobb szerverek rendelkezzenek egyértelműen meghatározott felelős üzemeltetőkkel, s önálló szabályzattal;
- a fejlesztési tervek és a fejlesztések biztonsági szempontból is legyenek átgondoltak;
- biztosított legyen a rendszeres tájékoztatás, oktatás és gyakorlás;
- átgondolt, következetes és gondosan végrehajtott mentési rend kell;
- legyen terv a rendkívüli eseményekre (katasztrófa terv);
- vezessünk gépkönyveket, naplózzunk minden privilegizált accounttal kapcsolatos és rendkívüli eseményt (itt részben automatikus *(online)*, részben manuális naplózást kell végeznünk);
- gépkönyveket, naplófile-okat gondosan archiváljuk, rendszergazda váltás esetén fordítsunk figyelmet az átadásra.

Alapvető, hogy egy intézményen belül főbb vonalakban egységes biztonsági politika érvényesüljön, ez legyen összhangban a társintézményekével, partnerekével, s legyen összhangban a használt globális hálózatokéval is.

Az informatikai menedzsment biztonsági feladatai nem közömbösek a felhasználók számára, így némi betekintés kívánatos e területre. Példák a menedzsment feladataiból (a teljesség igénye nélkül):

- napi, heti, havi mentés, visszaállítási gyakorlat (utóbbi persze nem napi rutinfeladat);
- logfile-ok, rekordok ellenőrzése;
- naplózás;
- nem használt felhasználói bejegyzések *(dormant account)* felülvizsgálata, törlése;
- rendkívüli események kivizsgálása;
- jelszó menedzsment (jelszó nélküli accountok felszámolása);
- felhasználók figyelmeztetése rossz jelszó használat stb. esetén;
- vírusellenőrzés;
- rutin és szúrópróbaszerű ellenőrzések;
- hibák elhárítása, kiküszöbölése;
- hálózatbejárás;
- szünetmentes tápegységek ellenőrzése;
- tájékoztatás, figyelmeztetés, riasztás stb.

Időszakonként a rendszer teljes átvilágítása válhat szükségessé, ez mindig megteendő súlyosabb biztonsági események után.

Meg kell jegyezni, hogy a fenti követelményeket sehol sem teljesítik maradéktalanul, de ez inkább sajnálatos, mind követendő. Az ésszerű biztonsági politika nem teszi lehetetlenné a működést, betartása több előnnyel jár, mint hátránnyal.

## ISMERI SAJÁT MUNKAHELYE INFORMATIKAI FELHASZNÁLÁSI ÉS BIZTONSÁGI POLITIKÁJÁT?

## 3. Fizikai biztonság

A számítógépek, adathordozók, hálózatok és ezek környezete sebezhető.

A veszélyforrások igen sokrétűek:

- lopás, szándékos rongálás;
- fizikai veszélyforrások, mint:
  - tűz;
  - víz, nedvesség (csőrepedés, billentyűzetre ömlő almalé, páralecsapódás);
  - napsütés, hideg-meleg;
  - por, füst, agresszív gőzök (dohányzás);
  - rengések (földrengés, járműforgalom);
  - villámlás, elektromos kisülések;
  - elektromos hálózat zavarai (rossz földelés, áramingadozás, áramkimaradás);
  - statikus elektromosság;
  - mechanikai sérülések;
  - rágcsálók, ízeltlábúak (vezetékek átrágása, érintkezési zavarok, rövidzárlat);
  - . . .

Valószínűleg a fizikai veszélyforrások okozzák a legtöbb üzemzavart, kárt (eltekintve a hardver és szoftver hibáktól), s a legnagyobbakat is. A védekezés a fizikai károk ellen a legnehezebb és a legköltségesebb. Emellett minden védelem alapja a számítógépes eszközök és környezet fizikai védelme. Pl. hiába mentünk, ha a mentési média károsodik.

A fizikai védelemnek nyilván sok közismert módja van, valamint a védekezés nagyon helyspecifikus, s terjedelmi okokból is elnagyoljuk e kérdés tárgyalását. Csak néhány dologra szeretnénk felhívni a figyelmet:

- illetékteleneket ne engedjünk szervereink, fontosabb berendezéseink közelébe, védjük eszközeinket és az adathordozókat lopás és szándékos károkozás ellen;

- a mentést (ill. a hordozó médiát) biztonságos helyen (esetleg több példányban), ne a számítógép mellett tároljuk;

- a mentést, archivált anyagainkat fizikai hatásoktól védett helyen tároljuk és/vagy rendszeresen ellenőrizzük, hogy nem érte-e őket károsodás;

- a különlegesen fontos berendezéseinket mindig zárt helyen, ne ablakok, fűtőtestek, vízvezeték szerelvények közelében üzemeltessük, tároljuk;

- a hálózat fizikai védelmére hívjuk fel a figyelmet, különös tekintettel az új dolgozókra és a takarító személyzetre (a költözködés, tatarozás gyakran okozza a hálózat sérüléseit);

- robusztus megoldásokat alkalmazzunk (pl. a vékony Ethernet igen sérülékeny, de megfelelő fali csatlakozók hatékonyan növelhetik a biztonságot);

- dohányzást ne engedjünk meg számítógépes környezetben;
- tartsuk tisztán, pormentesen környezetünket, védjük floppy és CD lemezeinket portól, piszkolódástól;
- adathordózókat le- (és el)zárva tartsunk;
- adatok mozgatására (kellő sávszélesség esetén) még mindig a hálózat a legpraktikusabb;
- működő gépbe ne nyúljunk, ne csatlakoztassunk hozzá berendezéseket (nyomtatót, szalagos egységet stb.);
- a száraz levegő, a műszálas anyagok elektromos kisüléseket okozhatnak (egy műszálas padlószőnyeg állandó bajok forrása lehet);
- a földelésekre mindig nagy gondot fordítsunk;
- használjunk megbízható szünetmentes és áramkondicionáló, túlfeszültség ellen védő berendezéseket, s ezek karbantartásáról, ellenőrzéséről ne feledkezzünk el (általában 2-5 évente telepcserére szorulnak);
- a vezetékeket (mind kommunikációs, mind erősáramú) úgy vezessük, hogy ne legyenek a közlekedési utakban, kerüljük a feleslegesen hosszú vezetékeket;
- gondosan dokumentáljuk, vezessük térképre vezetékeinket;
- a fizikai védelmet rendszeresen ellenőrizzék a hálózatüzemeltetők és mi magunk is;
- mindig ismerjük meg új berendezéseink karbantartásának módját, s az ésszerűség határán belül törekedjünk annak betartására;
- ipari környezetben ne irodai, hanem ilyen környezetre tervezett berendezéseket használjunk (pl. ipari PC-ket);
- biztonsági (behatolás, lopás, betörés, füst, tűz) érzékelőket általában célszerű a számítógép-hálózattal együtt telepíteni;
- alkalmazzunk beléptető/hozzáférési rendszereket (pl. smart card alapú megoldásokat), számítóközpontok, szerverszobák, számítógépes laborok stb. esetében kövessük nyomon ki, mikor, meddig, mit, mire használt;
- hasonlóan biztosíthatunk szervereket, nyomtatókat stb. (a használatot is mérve);
- hálózatunk WAN, GAN kapcsolatai rendelkézzenek tartalék *(backup)* vonallal, ill. legalább két független kapcsolatunk legyen (melyek pl. az Internet felé különböző nyomvonalon haladnak és különböző elérési pontokkal rendelkeznek). Az Internet esetén rendszerint az egyetlen kritikus szolgáltatás a levelezés. Erre backup vonalként akár analóg kapcsolt telefonvonal is szolgálhat (csak a rövid üzeneteket - pl. 10000 byte határig - átengedve hatékony és nem is túl költséges).

## 4. Megbízhatóság

A megbízhatóság alatt a hardver, a perifériák és a szoftver elvárható szintű üzemképességét, használhatóságát, ill. hibátlan működését értjük. Tapasztalataink szerint a legtöbb hibát, problémát nem a szigorúan vett biztonsági hiányosságok, vírusok, ellopott jelszavak okozzák, hanem a hardver és a szoftver hibák, hibás installálás, véletlen törlés, nem kielégítő karbantartás, rosszul tervezett, toldott-foldott hálózat. Más biztonsági eseményeket is kiváltanak, vagy ilyenekben közrejátszanak a fent említettek. A biztonság alapja a megbízható hardver és szoftver. A megbízhatóság szorosan összefügg a menedzsment és a fizikai biztonság helyzetével. E kérdéskör annyira szerteágazó és helyspecifikus, hogy az alábbiakban csak pontokba szedve emelünk ki néhány kérdést, ill. útmutatást adunk:

**A megbízhatóság alapja:**

- a képzettség és gondosság, mind a menedzsment, mind a felhasználók részéről;
- a gondosan kiépített, dokumentált, menedzsment és kontroll eszközökkel ellátott hálózat;
- a megbízható szervizháttér, egységes, jól integrált rendszerek;
- a fizikai biztonság megteremtése alapvető, enélkül biztonságot nem remélhetünk;
- dedikált berendezések, feladatok/szolgáltatások szétosztása növeli a biztonságot, bár nehézségeket is teremt, ugyanis több berendezést kell ellátnunk;
- törekedjünk az egyszerűen kezelhető, karbantartható, jól dokumentált (szükség esetén magyar dokumentációval rendelkező) termékek használatára;
- automatizáljuk a mentési, áram-kimaradási, menedzsment stb. funkciókat;
- robusztus technológiát alkalmazzunk;
- vezessünk gépkönyveket a javításokról, fontosabb változtatásokról;
- dokumentáljuk, hogy a konfigurációs file-okban és hasonlókban ki, mit, mikor és miért változtatott.

**A hardver megbízhatóságának alapja:**

- vállalati környezetben szinte mindig kifizetődőbb egységes *brandname* márkák alkalmazása a *noname*-ekkel szemben, így ezeket részesítsük előnyben;
- szerver feladatokra szerver kiépítésű/rendeltetésű berendezéseket célszerű alkalmazni;
- kellő tartalékot (skálázhatóságot) biztosítsunk a méretezésnél;
- állítsunk be tartalék eszközöket (elsősorban *'meleg'* tartalék javasolt, azaz folyamatosan elérhető, használt, de adott kiesett funkciók átvételére képes gép);

- technikában nem kifutó, hanem már érett, de még terjedő, felfutóban lévő, de már széles körben elterjedt technikát alkalmazzunk.

Számos hardver és szoftver technika használatos fokozott hibatűrés biztosítására (redundáns adattárolástól szerver tükrözésig), a hibák figyelésére és előrejelzésére, az egyszerű (esetleg működés közbeni) javíthatóság biztosítására.

A szoftverek biztonsága sokkal összetettebb kérdés. E tárgykört nem igazán lehet lefedni néhány tanáccsal. Inkább csak példaként néhány megjegyzés:

- házilag összetákolt szoftverek kétes értékűek állandó, folyamatosan jelentkező igények teljesítésére;
- márkás vagy közismert szabad szoftvereket alkalmazzunk;
- ha lehet adaptáljunk és ne fejlesszünk;
- csak jól dokumentált szoftvert használjunk;

Az alkalmazott szoftverek esetében szintén fontos azok gondos összehangoltsága, itt is törekednünk kell az egységesítésre, összhangra. A szoftverek kiválasztása, installálása, konfigurálása, *update*-je és *upgrade*-je jelentős támogatási igényt követel, mind a felhasználók, mind a menedzsment részéről.

A hálózatok megbízhatósága majdnem olyan összetett kérdés, mint a szoftvereké. De vannak egyszerű ökölszabályok (itt csak a fizikai szint kérdéseire kitérve):

- 'strukturált' hálózatot, árnyékolatlan sodrott érpárt, részben üvegszálat alkalmazunk;
- külső hálózatban vagy üvegszálat, optikai, mikrohullámú átvitelt részesítsünk előnyben, vagy kisebb sebességű technikát alkalmazzunk;
- mindig komoly (neves, referált) hálózatépítő céggel dolgoztassunk, adott esetben rendszerintegrátort alkalmazzunk;
- korszerű hubokat alkalmazzunk, ilyenekre térjünk át;
- alkalmazzunk túlfeszültség (pl. villám) elleni berendezéseket;
- a földelésekre nagy gondot fordítsunk, a földeléseket szakember vizsgálja felül;
- a hálózat nyomvonal vezetése, méretezése kritikus kérdés;
- a hálózati vezetékek védett csatornákban fussanak, zárható kábelrendezőket alkalmazzunk;
- a hálózati berendezések mindig a lehető legegységesebb típusúak, márkájúak legyenek, mindig kiváló minőségűek;

A kábeleink, a csatlakozóink, a berendezések portjai, a lengőkábelek áttekinthetően és közérthetően legyenek címkékkel ellátva. Mindig tüntessük fel, hogy egy helyiségbe, kábelcsatornába belépő kábel merre halad, merre hagyja el a helyiséget, honnan érkezik.

Persze ez többe kerül, mint a legolcsóbb út. A kapott funkcionalitás, bővíthetőség, fejlesztési lehetőség és a biztonság arányban áll az ebből adódó többletköltséggel.

# 5. A mentés

A mentés a tárolt információról történő biztonsági másolat, vagy másolatok készítése. Rokon fogalom az archiválással, bár a mentés fogalma ennél általánosabb, mert ekkor a még használatban lévő adatokról is készítünk biztonsági másolatot, sőt inkább ezen van a hangsúly. Az archiválás esetén szinte kivétel nélkül relatíve olcsó, off-line (kivehető) adathordozóra készül másolat. Archiválás esetén a cél az esetleges visszakeresés, míg a mentés esetén az elveszett sérült adatok helyreállításán van a hangsúly. Az alábbiakban csak a mentéssel foglalkozunk, de az elmondottak nagy része alkalmazható az archiválásra is (a két fogalmat gyakran nem is különítik el, szinonimként alkalmazzák).

A mentés mind a felhasználók, mind a rendszergazdák fontos tennivalója, de az utóbbiak egyik legfontosabb kötelessége is. Mind a felhasználóknak, mind a rendszergazdáknak mentési-visszaállítási stratégiával kell rendelkezniük, s a többfelhasználós rendszerek esetében írásban rögzített (és az érintettek előtt ismert) mentési-visszaállítási politikával is. A visszaállítás reális esélye nélkül a mentésnek sok értelme nem lehet, ezért a következőkben több esetben a mentés és visszaállítás helyett csak a mentést említjük.

Normális esetben a számítóközpontok rendszeresen mentik az általuk üzemeltetett szerverek, nagygépek adatait, sok esetben a felhasználók munkaállomásaiét is. A rendszergazdák, ill. nagyobb helyeken az ún. *backup operátorok* felelősek az adatok helyreállíthatóságáért. A felhasználók mindig tájékozódjanak a helyi mentési politikáról, de legfontosabb adataikat maguk is mentsék.

A visszaállítás kulcskérdés, méghozzá olyan feladat, amit tesztelni/gyakorolni kell (számítógép-központokban az ilyen gyakorlatot 'katasztrófa gyakorlatnak' nevezik, s végrehajtása része a mentési politikának). Sok kellemetlenség adódhat, ha csak akkor derül ki valamely adat visszaállíthatatlansága, amikor az eredetije már elveszett.

**Néhány fontos fogalom:**

| | |
|---|---|
| **Full backup** (teljes backup) | - a rendszer minden adatának (azaz felhasználói adatok, rendszer, hozzáférés stb.) mentése. Hetenként, de legalább havonként illendő egy teljes mentést végezni. |
| **Incremental backup** | - az előző backup után bekövetkezett változások mentése. Rendszerint napi feladat. |
| **Partial backup** (részleges backup) | - egyes adatok, adatcsoportok teljes mentése. |
| **Zero day backup** | - a rendszer induló állapotának mentése. |

**Útmutatók és tanácsok:**

- Rendszeresen mentsünk, legyen havi, heti, szükség esetén napi mentésünk. A napi, heti, havi stb. mentéseket egymástól függetlenül végezzük.
- Az egymást követő napi, heti, ... mentések rendszerint inkrementális mentések, de hetenként, havonként végezzünk független teljes mentést. A mentést addig őrizzük meg, amíg szükség lehet rá (ennek idejét nem könnyű felmérni: egy újabb mentés nem teszi szükségtelenné a korábbiak megőrzését!).
- A teljes mentést legalább két példányban végezzük.
- Legalább két fizikailag különböző helyen tároljuk mentéseinket (lehetőleg ne egy épületben).
- Olyan médiára mentsünk, ami szokásos s a jövőben is elérhető, hogy adatainkat később is visszaállíthassuk. Új médiára csak nagy körültekintéssel térjünk át.
- A mentési kapacitást méretezzük túl.
- Bizalmas információról készíthetünk titkosított (kódolt) mentést is. Vigyázzunk, hogy ez esetben is garantált legyen a visszaállítás lehetősége. Csak különösen indokolt esetben éljünk ezzel a lehetőséggel, s ne a teljes mentést, hanem annak kritikus részeit titkosítsuk.
- Biztonságos helyen tároljuk a mentéseinket (tűztől, víztől, erős elektromágneses hatásoktól, lopástól stb. védve).
- Mindig gondosan adminisztráljuk a mentést (mikor, mit, mire stb. mentettünk).
- Legyen két független eszköz a visszaállításhoz (vagy ha csak egy van, legalább tudjuk, hogy honnan kérjünk kölcsön, ha az az egyetlen meghibásodott).
- Ahol csak lehet automatizáljuk a mentést, többszintű mentési politikát alkalmazzunk.
- Ne idegenkedjünk az ún. *hardcopy* mentésről, azaz fontos adatainkat, a rendszer visszaállításhoz szükséges információkat (pl. konfigurációs file-ok tartalmát) nyomtatott formában is őrizzük.
- Vigyázzunk, ne használjunk elhasználódott médiát mentésre, fordítsunk gondot a mentő eszköz megbízható működésének ellenőrzésére. A szalagokat nem szabad túl sokszor felhasználni. Egyes helyeken egyáltalán nem használják mentésre kétszer ugyanazt a szalagot, de ez túl drága megoldás. A márkás szalagok több százszori teljes újraírást is kibírnak (a szalagos meghajtótól, tárolási körülményektől függően), de a magunk részéről ennél gyakoribb selejtezést javaslunk.
- Az adataink értéke szerint mentsünk.

**Mentési médiák:**

Az átlagos felhasználó számára a hajlékonylemezek megfelelnek (archiválásra már nem, de a legfontosabb adatok mentésére igen). Egy második merevlemezes egység, vagy központi erőforrások (szerverek) általában szintén használhatók, de kritikus anyagainkat mentsük off-line médiára is.

A szerverekre töltést azonban a helyi rendszergazda ellenezheti, különös tekintettel arra, hogy nagy diskquoták (tárkorlátozások) esetén vagy quoták hiányában sokan előszeretettel kukásedénynek tekintik a szervereket. A fileszerverek használata mindemellett igen kényelmes (megbízhatóságuk is általában nagyságrenddel vagy többször nagyobb a munkaállomásokénál), valamint az itt tárolt anyagokról amúgy is rendszeresen mentésnek kell készülnie. Néhány fős munkacsoportnak is érdemes file-szervert üzemeltetni, már csak háttértárolónak és mentőeszköznek is. Szerverekről történhet munkaállomások mentése is (bár ez DOS/Windows környezetben nem mindig oldható meg kényelmesen).

A nagyobb tömegű mentési feladatokra ma a szalagos egységek a legmegfelelőbbek. A szalagok olcsók, többször felhasználhatók, egyszerűen kezelhetők, léteznek kellően nagy kapacitásúak. Gondosan érdemes kiválasztani az egység típusát (a különféle DAT kazettás egységek a legáltalánosabbak). Nincs ok hinni azoknak, akik a szalagokra mentés hibáit hangoztatják. Ma még ár/teljesítmény és kényelem terén mindenképpen felülmúlják az optikai, magneto-optikai technikákat, de archiváló egységnek a CD-R ígéretes.

A különféle cserélhető merevlemezes, vagy nagy kapacitású floppy meghajtó egységek és hasonlók ma általában nem kifizetődőek, mellesleg nem is elterjedtek.

A mentési médiák és berendezések ügyében forduljunk szakemberhez.

**Mentés a gyakorlatban, tapasztalatok:**

El kell mondanom azonban, hogy lényegesen kevesebb intézményben találkoztam mentési politikával és kielégítő mentéssel, mint ahol ilyenről egyáltalán nem is beszélhettünk. Kielégítő gyakorlat ritka mint a fehér holló, túlzásba vitt mentési gyakorlattal még nem találkoztam. Általában senki sem veszi komolyan a mentést, amíg keserű tapasztalatokat nem szerez - sokaknak nem elég az egyszeri rossz tapasztalat sem.

Még egyszer megjegyezzük:

**A LEGTÖBB BAJ MEGELŐZHETŐ MEGFELELŐ MENTÉSSEL!**

## 6. A jelszó

Szinte minden többfelhasználós rendszer jelszót kér bejelentkezéskor *(login)* ill. kapcsolatfelvételkor. A jelszó használata számos más esetben is szokásos: képernyővédő, setup beállítások, rendszerindítás, partíciók, könyvtárak, file-ok, adatbázisok elérésénél, programok indításánál stb.

Gyakran **többszintű jelszavas védelmet** alkalmaznak, azaz egymás után több jelszó kérést kell kielégítenünk. Pl. belépünk egy többfelhasználós rendszerbe: először a rendszer, utána az adatbázis menedzsment rendszer kér jelszót. A jelszavas védelem más módszerekkel kombinálható (pl. PIN kártya, ujjlenyomat ellenőrzés), ez az ún. **többfaktoros védelem**.

A jelszavas védelem olcsó, könnyen kivitelezhető, egyszerű, jól bevált és széles körben elterjedt módszer, számos gyengeséggel. Más védekezési módokkal kombinálva (pl. többfaktoros védelem) rendkívül hatásos.

Gyengesége elsősorban a felhasználók hanyagságában, tájékozatlanságában rejlik, másrészt rendszerint a teljes védelem egyetlen jelszóra alapozott, így ellopása, kitudódása katasztrófához vezethet. A legtöbb betörést a rossz jelszavak használata (lásd alább), vagy a jelszavak hiánya okozza. Egyes becslések szerint a behatolások több mint 80 %-ánál ez az ok. Másrészről a jelszavak sokszor nem biztonságos módon tárolódnak a rendszerekben, haladnak át a számítógép vonalakon, hálózatokon. 'Nem biztonságos'-on értjük a **titkosítatlan jelszavak** használatát, azaz ha a jelszó lehallgatható vagy kinyerhető a rendszerből.

Fontos tudni, hogy a(z operációs) rendszerek a jelszavakat általában nem tárolják, hanem egyutas módon titkosítják, s a titkosított jelszavakat hasonlítják össze.

A fentiek alapján kijelenthetjük, hogy a jelszavak használata kulcsfontosságú biztonsági kérdés. A csekély biztonsági igényt követelő rendszerek (pl. az akadémiai szféra rendszerei) és az Internet védelme alapvetően az egyszerű (egyfaktoros, egyszintű) védelemre és nem biztonságos utakra *(biztonságos úton olyan kommunikációs csatornát és adatforgalmat értünk, mely kellően biztonságos - azaz nehezen hallgatható le, az adatok módosíthatóságának esélye csekély, s az illetéktelen hozzáférés észlelhető stb.)* alapozódik, ilyen rendszerek esetében ez tekinthető arányos védelemnek. Azonban az Internet túlnőtt az akadémiai felhasználáson, így a **biztonságos utak** ill. az ún. **egyszer használatos jelszavak** előtérbe kerültek.

A problémák zöme mégis az alábbiakból fakad:

- a felhasználó nem érti, miért kell neki jelszavakat használnia;

- miért nem oszthatja meg másokkal a jelszavait;

- nem gondol arra, vagy nem gondos eléggé ahhoz, hogy nehezen kitalálható jelszavakat használjon;

- és ha már nem triviális jelszavakat használ, akkor elfelejti a jelszavait;

- ezek után legközelebb felírja jelszavait (nem mindig tekinthető ez rossz megoldásnak, de ha egy nyilvánosan elérhető titkosítatlan file-ba teszi őket, az már nem az igazi).

Sok esetben a felhasználó nem ismeri a file engedélyek megadásának módját, s csak a jelszó átadásával tudja más részére átadni a hozzáférést.

Mint mindig, most is megjegyezzük, hogy a rendszeres mentés a legfontosabb kiegészítő védelem. Így legalább adataink elvesztésétől megóvhatjuk magunkat.

Az alábbiakban pontokba szedve rövid útmutatót adunk néhány, jelszavakkal kapcsolatos kérdésben.

## Útmutató a helyes jelszó használathoz:

- Ún. 'jó' jelszavakat használjunk *(lásd alább).*

- Minden rendszerhez különböző jelszót használjunk (legalább néhány karakterben különbözzenek a jelszavak), többszintű védelemben ne használjunk egyező jelszavakat.

- Csak titkosított formában tároljunk jelszavakat.

- Legyünk tisztában vele, hogy rendszereink hogyan tárolják, továbbítják jelszavainkat.

- Ha több jelszót használunk, akkor dolgozzunk ki magunknak jelszó használati, képzési politikát.

- Rendszeresen változtassuk jelszavainkat (de nem érdemes gyakran).

- Ne osszuk meg mással az accountunkat, ne adjuk át másnak jelszavunkat, ne használjunk közösen accountokat (ennek használatára még nem találkoztunk elfogadható indokkal).

## Útmutató helyes jelszó választáshoz:

A jó jelszó
- nehezen kitalálható,
- könnyen begépelhető,
- könnyen megjegyezhető,
- igény szerint 5-10 karakter hosszú,
- tartalmaz betűket, számokat és/vagy írásjel karaktereket.

Azt hiszem nem kell sok képzeleterő jó jelszavak kitalálásához.

## Egyéb problémák, kérdések:

Számos esetben találkozunk program generálta jelszavakkal, melyek megjegyezhetetlenek, esetlenek. Néhány esetben az ilyen jelszavak megváltoztatását a rendszer nem engedélyezi. A megváltoztathatatlan jelszavak csak többszintű jelszavas védelem egyes szintjein fogadhatók el - legalábbis e sorok írója szerint.

Tisztában kell lennünk azzal, hogy rendszereink gyakran úgy konfiguráltak, hogy bizonyos időközönként meg kell változtatnunk jelszavainkat, s jelszavaink nem lehetnek a korábban használtak. A rendszer nem engedi meg bármilyen jelszó megadását (minimális hossz, megkövetel kis és nagybetűt stb.). Számos rendszer megengedi hosszabb jelszó használatát is, mint amit figyelembe vesz (azaz pl. csak az első 8 karaktert veszi figyelembe).

Ritkán előfordul, hogy jelszavunkat a rendszer visszaírja a monitorra. Ennek okaira itt nem térünk ki, de ilyen esetben feltétlenül forduljunk az illetékesekhez segítségért.

A lehallgatásról külön fejezetben foglalkozunk (*lásd a 9. fejezetet).*

Fontos megemlítenünk, hogy egyes rendszerek (pl. Unix) megkülönböztetik a kis és nagybetűt. Ilyenkor a 'Caps Lock' gomb véletlen lenyomása megtéveszthet bennünket és nem tudjuk begépelni a jelszavunkat. Még gyakoribb, hogy a billentyűzetvezérlőnk magyar ékezetre van állítva, s emiatt vagyunk sikertelenek.

Érdemes arról is szólni, hogy a jelszó lopások *(itt nem valódi lopásról van szó, a tolvaj nem tudja meg a jelszavunkat, csak megváltoztatja, inkább account lopásnak nevezhetjük az ilyen eseteket)* jelentős része az őrizetlenül hagyott terminálok, az elfelejtett kijelentkezések miatt következik be.

## Jelszavak és az Internet

Az Internet biztonságát érintő legtöbb kritika a titkosítatlan jelszavak elterjedt és részben elkerülhetetlen alkalmazását illeti*. A titkosítatlan jelszavak inkább a helyi hálózatokon okoznak gondot, a lehallgatás itt a legkönnyebb és leggyakoribb. Az Internet biztonsága mindig és most is lépést tartott/tart a felmerülő igényekkel. Természetesen a kereskedelmi forgalom megjelenése hatalmas és hirtelen jelentkező igényeket támaszt.

* Vegyük azonban figyelembe, hogy egyrészről az TCP/IP protokollok (alsó réteg, azaz a hálózati IP, és transzport TCP és UDP) nem zárják ki, hogy a felső hálózati rétegek ill. az alkalmazások titkosítást alkalmazzanak (pl. HTTP helyett SHTTP-t), másrészt más rendszereken a titkosítatlan jelszavak használata épp így szokásos (pl. BBS-ek esetében - igaz, hogy a kapcsolt telefonvonalak lehallgatásának kisebb a veszélye).

## VÉDI ACCOUNTJÁT JELSZÓVAL? JÓ JELSZAVAKAT HASZNÁL?

## 7. Hitelesség és hitelesítés

Üzenetek, levelek, osztott dokumentumok és adatbázisok használata esetén fontos, hogy valóban a vélt személy küldte-e az üzenetet, végezte-e a módosítást, valamint illetéktelenek nem 'piszkáltak-e' bele az adatokba. Emellett fontos, hogy az adatok hitelességét ellenőrizni tudjuk, vagy kellő alapunk legyen abban megbízni.

A hitelességet legtöbbször az biztosítja, hogy csak az illetékes személy jogosult az adott művelet végrehajtására, pl. csak neki van hozzá elérési joga. Mindazonáltal a hitelesség nehezen igazolható csak ilyen módon, különösen ha többen is (esetleg illetéktelenül is) rendelkeznek az adott hozzáférési joggal.

Az operációs rendszerek, adatbázis-kezelők, levelező rendszerek jegyezhetik, hogy ki, mit, mikor csinált, de egyrészt ezeket sokszor be lehet csapni, másrészt nem mindig könnyű a visszaellenőrzés.

Ha elektronikus üzenetek hitelessége esetében gyanúnk merül fel, akkor telefonon vagy más módon rákérdezhetünk az üzenet szerzőjére, ellenőrizhetjük, hogy létező accountról érkezett-e az üzenet. A dokumentumok, üzenetek formája is árulkodhat.

A hitelesítésnek más, biztosabb - szinte tökéletes - módjai vannak. A megoldás kriptográfiai módszerek alkalmazása. A titkosított üzenetet megfelelő kódolás esetén csak a kulcs ismerője készíthette, a dokumentumról készült ellenőrző összeget kódolva a visszafejtés (kellő) nagy valószínűséggel csak a kódolt üzenet változatlansága esetén tehető meg. Sőt, elég csak az ellenőrző összeget kódolnunk, ezzel a hitelesítés (mind az aláírás, mind a belepiszkálás elleni védelem) megoldott. A keltezést az ellenőrző összegbe foglalva annak hitelességét is igazolhatjuk.

Az utóbbi időben a World-Wide Web terjedésével előtérbe került az ún. *Internet cache*-ek alkalmazása, azaz a már egyszer lehívott információk ideiglenes tárolóba történő helyezése, a rákövetkező esetleges lekérések gyorsabb megválaszolása céljából. Ilyen esetekben a dokumentum hitelességégének és aktualitásának kérdése élesen jelentkezik. E kérdéskörre a megoldások még nem teljesek. Tudnunk kell, mikor kell kikerülnünk a *cache*-eket.

A hitelességnek egy másik értelme is van: az Interneten elérhető dokumentumokat, programokat mikor fogadhatjuk el hitelesnek? valódi és helyes információkat tartalmaznak-e? a programok elvárásaink szerint viselkednek-e? Ez azonban már nemcsak számítógép-biztonsági kérdés.

### A számítógépes versus hagyományos aláírás és dokumentum hitelesítés

Megdöbbentő, hogy milyen kétkedéssel fogadják az elektronikus levelek hitelességét, míg pl. fénymásolt (faxolt) aláírásokat azonnal hitelesnek fogadnak el. Emellett számítógépes és/vagy pénzügyi szakemberek azt hiszik, hogy az elektronikus aláírás Magyarországon nem fogadható el jogi korlátozások miatt, de a faxolt aláírást el lehet fogadni. Valóban van számos ésszerűtlen jogi megkötés, de a

pénzügyi világban általában nálunk is alkalmazható a digitális aláírás (az más kérdés, hogy partnereink azt sem tudják, hogy eszik ezt vagy isszák). *(Lásd alábbi kis írásunkat: "Mi az a digitális aláírás".)*

A digitális aláírás gyakorlatilag az egyetlen jól bevált mód, mellyel egy teljes dokumentumról igazolni lehet nem csak annak hiteles aláírását, de a teljes dokumentum változatlanságát, azaz, hogy azt nem módosították az aláírása óta, valóban a keltezés idejében állították ki, stb. (s mellékesen a titkosságot is biztosítottuk).

Kódok, jelszavak, hitelkártya számok átküldésére a megfelelően titkosított, digitális aláírással ellátott üzenetek nyilván alkalmasabbak, mint a telefon, a fax vagy a csigaposta. Sőt, ez utóbbiak titkosítás nélkül nem is tekinthetők alkalmasnak.

Bár üzleti, vállalati rendszerek biztonságával nem kívánunk itt foglalkozni, fontos megjegyeznünk, hogy az - üzleti és hivatalos - elektronikus adatcserére *(Electronic Data Interchange - EDI)* nemzetközi (ENSZ) és US szabványok széles körben elfogadottak.

**Mi az a digitális aláírás?**

Rögtön előrebocsátjuk, hogy nem a közönséges aláírásunk digitalizált változata. A digitális aláírás egy olyan titkosított karaktersorozat (vagy más információ), melyet igen nagy valószínűséggel csak a küldő ('aláíró') kódolhatott, s ez magából a kódolásból következik. Keltezést (dátumot, pontos időpontot), sorszámot (a visszajátszás megakadályozására), a küldött üzenetből készült ellenőrző összeget stb. tartalmazhat. A részletek iránt érdeklődőknek **A. S. Tannenbaum: Számítógép-hálózatok** (605-610. old.) című könyvét ajánljuk *(lásd a füzet végi irodalomjegyzéket).*

**Pretty Good Privacy (PGP) és Privacy-Enchanced Mail (PEM)**

A PGP és PEM programok a titkos és hiteles hálózati kommunikációt szolgálják, nyilvános kulcsú kriptográfiára támaszkodva.

A számítógépes üzenetek titkosításának de facto szabványa ma a PGP. Bővebb információt az alábbi URL alatt kaphatunk róla:

*http://draco.centerline.com:8080/~fran1/pgp/*

Lásd még:

*http://www.cs.indiana.edu/ripem/dir.html*
*http://www.rsa.com*
*http://www.ifi.uio.no/~staalesc/PGP/home.html*
*http://www.cisc.ohio-state.edu/txt/faq/usener/pgp-faq.html*
*gopher://gopher.mek.iif.hu:7070/00/porta/szint/muszaki/szamtech/wan/pgp.hun*

Mindenekelőtt az NIIF füzetsorozat I/7. **"Kapcsolattartás e-mail útján az Interneten"** című füzetét ajánljuk az ide és a következő fejezetre vonatkozó további tanulmányként.

## 8. Névtelen levelek és üzenetek

A következőkben hamis leveleknek nevezzük a szakirodalom által *'pseudonym'*-nak (angolul *'fake mail'*, ill. *'forged mail'*-nek) ismert leveleket, melyeket hamis címzéssel (nem létező címmel vagy más nevében) adtak fel, s a névtelen leveleket is ide értjük.

Sok levelezőrendszerben (pl. az Internet alapvető levelezőrendszerében) könnyű, vagy legalábbis lehetséges hamis levelet küldeni. A levelező rendszerek átjárói is lehetővé teszik, hogy olyan rendszerből kapjunk üzenetet, mely gyenge kontrollal rendelkezik a feladó hitelesítésére.

A névtelen levelek egy része gyalázkodó, sok vizet nem zavar, de bosszúságot okozhat. A névtelen levelek más részénél a feladó csak az anonimitását akarja megőrizni, rossz szándék nélkül. Mindenesetre a névtelen levélküldés nem tekinthető kedvező jelenségnek, de más nevében hamis levelet küldeni megengedhetetlen. Ilyenkor érdemes erre felhívni az illetékes postamester vagy rendszergazda figyelmét és segítségét kérni - ez közérdek.

Nagyobb gondot okoznak a mások nevében küldött üzenetek: ilyenkor az üzenetek tartalma, stílusa stb. árulkodhat. Sok esetben a levél header vagy boríték (RFC 822 terminológia szerint) árulja el a feladás rendellenes voltát.

Nyilvánvaló mód a feladó hitelességének ellenőrzésére a rákérdezés, ill. a levél visszaküldése a feladónak. Lehetőleg persze ne e-mailen, hanem más csatornán tegyük ezt, e-mailen legfeljebb akkor, ha a feladó címe létezik, s tudjuk vagy ellenőriztük, hogy azt a jogos tulajdonosa használja.

A hamis levelek problémáját az üzleti, ill. bizalmas levelezésben legjobban a digitális aláírással küszöbölhetjük ki. Az Internet levelezésre is megjelentek szabványok a titkosság és a feladó hitelesítés biztosítására.

A névtelen és hamis üzenetek kérdése alapjában véve egyezik a hamis levelekével.

Rokon probléma a véletlen levélküldés téves címre vagy címekre. Némileg kellemetlen érzése lehetett annak a hölgynek, kinek szerelmes levelét vállalatának kétszázötven dolgozója megkapta. Az esetlen Compuserve és más hasonló címeknél nem ritka, hogy rossz gépeléssel valódi címet találunk el. Levelező szoftverek (saját magunk által írt) makrói szintén okozhatnak tréfákat.

# 9. Hálózatok lehallgatása

A hálózatokon, kapcsolt vonalakon haladó adatforgalom többé-kevésbe könnyen lehallgatható. Különösen a helyi hálózatok adatforgalma hallgatható le könnyen, az itt szokásos üzenetszórásos technika jóvoltából (egy hálózati szegmens* minden egyes munkaállomásához a többi munkaállomás minden üzenete eljut). Az átlagfelhasználó rendszerint nem is sejti, hogy a helyi hálózatok milyen könnyen lehallgathatók. E védtelenség a helyi hálózatok eredeti rendeltetéséből is származik, hiszen ezeket csoportmunkára szánták, ahol a lehallgatás nem jelent komoly rizikó faktort. Az analóg kapcsolt (telefon) vonalak lehallgathatósága közismert, de csak a központokban lehet nagyszámú vonalat egyszerre lehallgatni, így itt a veszély a helyi hálózatokénál sokkal kisebb - de fennáll.

Számos adatátviteli mód nehezen hallgatható le (ISDN, GSM, optikai átvitel, vagy a szinte lehallgathatatlan szórt spektrumú átvitel), de a tökéletes megoldást csak a teljes adatforgalom titkosítása jelentheti. Akadémiai célú felhasználás ezt nem indokolhatja. Azonban a legfontosabb adatok (jelszavak, bizalmas üzenetek) titkosíthatók. Több operációs rendszer és hálózati alkalmazás vagy eleve titkosított formában küldi át a jelszavakat, vagy ún. titkosított, egyszer használatos *('one-time password')* jelszavakat használ.

A jelszavak titkosítása önmagában még nem megoldás, hiszen a titkosított jelszót elfogva, azt újra lejátszva beléphetünk egy rendszerbe anélkül, hogy a jelszót tudnánk. A mai rendszerek, ha már titkosított jelszavakat használnak, akkor alkalmaznak módszereket a titkosított jelszó újrafelhasználásának megakadályozására is. Itt nem akarunk ennek a technikai részleteibe bonyolódni.

Technikailag könnyű kivitelezhetőségének köszönhetően az utóbbi időkben a helyi hálózatok lehallgatása elterjedt. Szabadon elérhető, BBS-ekről, anonymous FTP helyekről letölthető szoftverek alkalmasak lehallgatásra, melyeket egyébként a hálózati menedzserek hálózatmonitorozására, a forgalom analizálására fejlesztettek ki. E szoftverek használata meglehetősen erőforrás-igényesnek számított, de ez már nem áll fenn, az utóbbi idők átlagos PC-i már képesek futtatni ilyen programokat. Így a lehallgatás széles körben elérhetővé vált. A hálózat kivitelezése, topológiája nagyban befolyásolja a lehallgatás lehetőségeit, azonban ez idáig a lehallgatás elleni védelem nemigen volt szempont a hálózattervezéskor. Szerencsére korunk új technikái, melyeket a nagyobb hálózati teljesítményigények miatt alkalmaznak, nagyban nehezítik a lehallgatást (pl. a *switching hub*-ok).

A hálózatok lehallgatása rendkívül jelentős, ez úton tömegével lehet jelszavakat illetéktelenül megszerezni. A védekezés nehéz, nagyon is nehéz lehet. Elvben vannak megoldások, de alkalmazásuk a gyakorlatban körülményes. A legfontosabb, hogy szarvashibákat ne kövessünk el:

- ne jelentkezzünk be távolról superuser vagy más kritikus jelszóval,
- ne küldjünk e-mailen, ne tároljunk file-ban titkosítatlan jelszavakat.

Sokat segíthet:

- a környezetünk, a hálózat gépeinek ellenőrzése, figyelemmel kísérése;
- már magának a problémának az ismerete is.

Alapvető megoldást a hálózatok megfelelő kialakítása, adott esetekben átszervezése, valamint bizonyos hálózatmenedzsment megoldások jelentenek. A probléma összetett, s csak összetett, önmagában nem teljesen hatékony eszközökkel védekezhetünk, melyek együttesen már hatásosak.

A jelszavak illetéktelen megszerzése munkaállomásokon elhelyezett ún. 'jelszó lopó' programokkal is könnyen megvalósítható. Ez lehet egy 'ál-login' program, mely először lejegyzi a jelszót, majd végrehajtja a valódi login procedúrát. Tökéletlen programoknál feléledhet a gyanúnk, de nyilván az ilyen program illetéktelen gépre kerülését kell elkerülni, ill. legalább kritikus accountokat (pl. superuser) potenciális támadásoktól védett gépről használjunk. Természetes a jelszavak leleshetők, rejtett kamerával is felvehetők, s a trükkök sorát folytathatnánk, sőt a fent említetteknél még rafináltabb lehallgató eljárások is ismeretesek.

* Szegmens alatt routereket, bridge-eket, switcheket csak a határain tartalmazó hálózatrészt értünk.

## 10. Vírusok, férgek, trójai falovak és egyéb programozott kórokozók

Az alábbiakban olyan programokkal, programkódokkal foglalkozunk, melyet ártó szándékkal (beleértve az illetéktelen elérést is) hoztak létre, vagy kísérletezésből, játékból születettek, de veszélyt jelentenek és kárt okozhatnak. Az ilyen kódokat *'vandalware'* szóval is illetik, mely roppant találó, bár nem elterjedt. E programok sajátos csoportját alkotják a **vírus**ok és a **férgek (worms)**, melyek sajátsága, hogy aktivizálódva reprodukálódhatnak, s egy rendszerben vagy számítógépek közt terjedhetnek. Bár számos más csoport is idetartozik, ezek közül csak a trójai falovakat (**Trojan Horses**) tárgyaljuk. Említjük a **bombák**at (**bombs**) és a **csapóajtók**at (hátsó ajtó - **trap door, back door**), melyek, mint az előzőek 'alkatrészei' érdekesek. Az egyéb csoportok jelentősége nem kicsiny, de nem a nyílt hálózatok (Internet, BBS-ek) esetében, vagy túl speciális kérdés lenne tárgyalásuk. A vírusokban, férgekben és trójai falovakban még két közös vonás van, ami a közös tárgyalásukat indokolja:

- a hasonló károkozás;
- az ellenük történő védekezés hasonlósága, mely a terjesztés- és terjedésbeli rokon vonásokból fakad.

### Vírusok

A vírusokra több definíció használatos. Szűkebb értelemben (mi mindig így használjuk) a vírus egy programkód, mely önállóan működésképtelen, melyet program vagy program információs file tartalmazhat, a program végrehajtásával aktivizálódik és replikálja magát, hozzáfűzi vagy beleírja magát más programokba.

A vírusokat rendszerint ártó szándékkal hozzák létre (bár kísérleti vagy játék célból is születtek). Általában az észrevétlen terjedés érdekében rejtettek, károkozásukon kívül nehezen vehetők észre (segédeszközök nélkül). Gyakran bombákat tartalmaznak, egyesek képesek más vírusokkal interakcióba lépni.

A vírusok nem hatásosak, ha nem kerülnek végrehajtásra. Ezért a másolás s minden más, végrehajtás nélküli tevékenység veszélytelen velük. Adatfile-t nyugodtan beolvashatunk rendszerünkbe (feltéve, ha nem tartalmaz program információt valamely végrehajtandó program számára). Léteznek vírusok ill. vírusszerű kreálmányok, melyek bootlemezről a bootkóddal aktivizálódhatnak, így fertőzött lemezről a bootolás veszélyes.

Hasznos tudnunk, hogy csak az egyfelhasználós rendszerek ellen bocsátottak szabadon vírusokat (PC-s DOS és Windows, Macintosh System, Amiga és Atari OS , ...). Unix-ra írtak, de csak kísérleti célból, VMS-re, mainframe-re nem ismeretes vírus (bár a szakirodalom említ ilyeneket, ezek nem vírusok a mi definíciónk értelmében). NetWare alatt futót soha senki nem írt. OS/2-re létezik. NT-re tudtommal nincs, a Windows 95 terén a szerző sajnos tájékozatlan. Olyan vírus sem ismeretes, amely több operációs rendszer alatt is működőképes lenne. Bár

többfelhasználós rendszerekre lényegében nincsenek vírusok, ez nem zárja ki, hogy DOS vagy Windows emuláció alatt vírusok nem aktivizálódhatnak, replikálódhatnak, sőt akár károkat is okozhatnak - pl. a Word makró vírusok -, de ezek operációs rendszer szinten már nem veszélyesek.

### Férgek

A férgek - ellentétben a vírusokkal - önálló programok. Máskülönben hasonlóak a vírusokhoz. Férget sokkal kevesebbet írtak mint vírust, s mivel ezek hálózaton át terjednek elsősorban, ezért a többfelhasználós rendszerek az elsődleges célpontjaik. Híres példa az Internet 1988-as féregfertőzése (az *Internet Worm*).

Az első férgeket kísérleti jelleggel, hasznos célra hozták létre. Céljuk az akkor szűkösen elérhető számítógépes erőforrások feltárása és kihasználása lett volna. A gondolat azóta is kísért, bár nem erőforrás, inkább információgyűjtés (pl. WWW-n - *vigyázat a WWWWorm nem féreg!*), hibaelhárítás és hálózatmenedzsment célból. Számos DOS-os féreg van, amit rendszerint vírusként emlegetnek.

A férgek potenciálisan nagyobb veszélyt jelentenek. Az ismert vírusok elterjedése hamar korlátokba ütközik, s a terjedési sebesség is kisebb annál, hogy ne lehetne hatékony riasztást és védelmet alkotni. Persze elvben egy féreg terjeszthet vírust is, s így már egy vírus is kemény dió lehet, de ezt az ötletet a vírusírók még nem használták ki. Mindazonáltal a mondottak a jelen pillanatban érvényesek, s nem elvi korlátok. Meglepő lehet, hogy az 1988-as *Internet Worm* eset óta nem következett be súlyos féregfertőzés az Interneten. Ez részben az 1988-as intézkedéseknek köszönhető, részben a szerencsének. Talán az Internet globális biztonsága lépést tart a támadókkal.

### A trójai falovak

A trójai falovak olyan kódok, programok, melyeket más programba rejtettek. Ilyen értelemben a vírusok is trójai falovak, de a trójai falovak nem feltétlenül vírusok. A trójai falovon inkább olyan programot szokás érteni, mely hasznos programnak látszik, vagy valamely más hasznos/ismert program preparált változata. Sokkal könnyebb trójai programot készíteni, mint vírust vagy férget, sokkal jobban is lehet álcázni, inkább a terjesztése nehézkes.

### Bombák

A bomba egy programkód, melyet valamely más program tartalmaz, s valamely feltétel (idő, esemény, vagy ezek kombinációja) hatására, vagy távvezérléssel 'robbannak', 'robbanthatók'. A fenti programozott kórokozók sokszor tartalmaznak ilyeneket, emellett szoftver másolásvédelemben, (shareware, bérelt stb.) szoftver hatástalanítására alkalmazzák. Ez utóbbi bombák csak az aktuális szoftver hatástalanítására szolgálnak.

## Csapóajtók

A angol nyelvű biztonsági irodalom a 'trap door' és a 'back door' kifejezéseket használja rejtett kiskapuk meghagyására, létrehozására, melyen az illegális behatoló bejuthat vagy újra visszatérhet a rendszerbe. Az angol 'trap door' egyik hétköznapi magyar megfelelője a 'csapóajtó', a 'back door'-é pedig a 'hátsó ajtó'. (Utóbbi félrevezető lehet, a 'hátsó ajtó' kifejezést a magyar nem ismeri. Talán a 'kiskapu' jó lenne, de ez érzelmi töltéssel bír. Így jobb híján maradunk itt is a csapóajtónál).

Csapóajtót hagyhat maga után a korábban legális eléréssel rendelkező felhasználó, egyszer illegálisan hozzáférést szerző személy, de csapóajtók telepíthetők trójai falovakkal, férgekkel és más módokon is. Sőt, programhiba, konfigurálási hiba folytán rendszerünkön eleve lehet csapóajtó. Értelemszerűen a rendszerek ellenőrzésének ki kell terjedni az esetleges csapóajtók feltárására is. Ilyen célra számos szoftvert írtak, de kényszerű okokból ezek operációs rendszer és alkalmazás specifikusak, valamint használatuk szakértelmet igényel.

## Védekezés

Az alábbiakban csak a vírusok elleni védekezéssel foglalkozunk, de nem azért mert a vírusok általunk kitüntettek lennének, hanem mert a védekezés más jószágok ellen is nagyban hasonló. Sőt, a vírusok a legártalmatlanabbak a fent említett lények közül. A mai napig nem írtak jelentős veszélyt jelentő vírusokat (a vírusírás messze elmarad a technikai lehetőségek mögött - nincs számítógépes megfelelője az AIDS-nek, az Ebolának és az influenzának). Mindemellett könnyen átláthatók és kivitelezhetők a védekezés módjai.

A védekezés alapja, hogy tudnunk kell, mi ellen védekezünk, milyen veszélyekkel nézünk szembe. A vírusnak valamely módon be kell kerülnie rendszerünkbe, így az izoláció teljes védelmet jelent, persze ilyen árat nem akarunk fizetni a hatásos védelemért. A következőkben a vírusvédelem legfontosabb teendőit pontokba szedtük. Először az egyéni (pl. otthoni) gépek, majd a helyi hálózatok felhasználóinak védelmével foglalkozunk. Megjegyezzük: tökéletes védelem nincs, de hatásos igen.

## (Helyi) hálózatba nem kapcsolt gépek esete

1. A vírusok adatvesztést, ill. a szoftver károsodását okozhatják. A szoftver károsodása is kellemetlen, hiszen sok esetben újra kell installálni rendszerünket, s ez pl. floppy-ról bosszantóan időigényes lehet, vagy önerőből nem is tudjuk végrehajtani. Adatainkat nagy baj nem érheti, ha rendszeresen mentettünk, s mentésünk nem vírusfertőzött. Elvben (volt rá példa a gyakorlatban is) vírus hardver károsodást is okozhat, de ennek veszélye rendkívül csekély. A szoftvereink visszatelepítése újrafertőzés nélkül lehetséges, hiszen installáló lemezeink írásvédettek (bár az

írásvédelem esetleges hardver hiba miatt nem garantált). Adataink vírusmentességét az biztosíthatja, hogy végrehajtható kód kell a vírusfertőzéshez, s ha ilyen nincs a lemezünkön, akkor fertőzöttek sem lehetnek adatállományaink. A kritikus adatállományainkat tartalmazó floppy lemezeinket - pl. egy Unixos gépen - átmásolva érintetlen lemezekre, azok vírusmentessége már garantált (igaz, hogy ez esetleg önerőből nem megy).

2. Víruskereső szoftverrel rendszeresen ellenőrizzük állományainkat, a kapott új állományokat is. A víruskereső szoftver legyen naprakész. Esetleg használhatunk ún. rendszerintegritást ellenőrző szoftvereket, de ez nem kötelező.

3. Legyünk óvatosak, ellenőrzött és ismert helyről szerezzünk be szoftvert (persze a kereskedelmi forgalmazás nem garancia).

4. Fogadjuk fenntartással, ha valaki pénzes vírusvédelmet, vírusvédelmi kártyát akar ránk sózni. Ezek önmagukban nemigen hatásosak, valamint vakriasztásokat okozhatnak.

5. Az OS/2 HPFS vagy az NT file-rendszer meglehetősen védett, Unix, VMS, NetWare ellen még nem került forgalomba vírus. Természetesen DOS-os (Mac stb.) vírusok előfordulhatnak ilyen file-rendszerekben is, csak nem képesek aktivizálódni a számukra idegen operációs rendszer alatt.

6. Ismételt vírusfertőzéseket a lemezeinken elfekvő vírusok okozhatnak.

7. Ha megtehetjük, a lemezeknél hatékonyabb mentő/archiváló berendezést szerezzünk be.

### Védekezés helyi hálózatokon

Helyi hálózatokon a fentiek közül minden eszközt alkalmaznunk kell, de ezeknél többet is, valamint a lehetőségeink is szélesebbek. Itt a fő cél a vírusbekerülés potenciális útjainak ellenőrzése, valamint a központi ellenőrzés. A tennivalók és lehetőségek:

1. Legyen vírusvédelmi politika, kapjanak vírusvédelmi útmutatást a felhasználók. Valósuljon meg együttműködés az érintettek között a vírusvédelemben (riasztás, tájékoztatás stb.).

2. Korlátozzuk a fertőzés útjait. Egyes helyekről kiszerelhetjük a floppy meghajtókat, sőt *remote boot*-tal diszknélküli üzemmódot használhatunk.

3. Szerverekről futtassuk alkalmazásainkat.

4. Használjunk központi file-szervereket és központi mentést, a mentéseket és a file-szerverek állományait ellenőrizzük, a file-szerverre másolt vagy módosított program azonnal kerüljön ellenőrzésre.

5. Ne DOS/Windows környezetet alkalmazzunk, ha lehetőségünk van másra.

Ha a fentiek alapján megfelelő gondossággal járunk el, a vírusfertőzéseket gyakorlatilag kiküszöböljük. Ha nincsenek kritikus alkalmazásaink (nem lehet munkaidő kiesés), akkor a helyi hálózatokon annyi baj sem lehet, mint az otthoni felhasználóknál, hiszen a visszaállítás a file-szerverekről pillanatok műve. (**Persze rosszul menedzselt rendszerekre ez nem áll!!!**).

A tapasztalat azt mutatja, hogy az áttérés a helyi hálózatra az egyedi PC felhasználásról, lényegesen csökkentheti a vírusfertőzések számát. Ez annak köszönhető, hogy nem fekszenek el vírusok hajlékonylemezeken, az ellenőrzés kiterjed a felhasználók állományaira, a file-ok nagy része megfordul a központi file-szervereken, a vírusvédelmi szoftver szétosztása és frissítése gyorsabb és szélesebb körű, a szoftverek telepítése tiszta forrásból történik. Bár a hálózat bevezetése számos új biztonsági probléma forrása, itt egy példa arra, hogy a biztonsági problémák megoldásában is lehet szerepe.

## 11. BBS-ek és anonymous FTP helyek

Mind az üzemeltetők, mind a felhasználók számára sok biztonsági problémát vetnek fel a szabad (nyilvános) elérésű archívumok, mint pl. BBS-ek és anonymous FTP helyek. A gondok nagy része csak az üzemeltetőket érinti közvetlenül, ezekkel itt nem foglalkozunk.

A problémák egyik fő forrása, hogy e helyek vírusok és más programozott kórokozók terjesztői lehetnek. A nevesebb FTP helyek archívumai, cégek *support* FTP helyei nagyon jól ellenőrzöttek, gondosan megválogatják, hogy honnan kerülhetnek ide programok, valamint az üzemeltetők minden tőlük telhetőt megtesznek az ellenőrzésre. Tökéletes védelem azonban nincs, a vírusok ellen a szigorú ellenőrzés még csak hatásos, de trójai falovak időnként felbukkannak.

A felhasználó részéről a védekezés a következő lehet:

- nem tölt le programot;
- a programokat izolált környezetben teszteli (karantén);
- gondosan tesztel vírus azonosító szoftverekkel;
- szoftvert csak hivatalos disztribúciós helyéről vagy ennek hivatalos (vagy más szempontok miatt biztonságosnak tekintett) tükör *(mirror)* helyeiről tölt le.

Látható, hogy csak az utolsó pont az, amit igazán követhetünk. Megjegyezzük, hogy a vírusellenőrzést nevesebb archívumok, disztribúciós helyek esetén nem tartjuk elengedhetetlennek. A vírusfertőzések elenyésző töredéke vezethető vissza anonymous FTP-ről letöltött file-okra.

A nyilvános elérésű helyekhez hasonló a helyzet a különféle helyi archívumokkal. Sajnos általános útmutatót nem lehet adni arra, hogy mely archívumok tekinthetők biztonságosnak, s melyek nem.

Egyes archívumokba bárki tölthet fel file-okat. Ha ezek az állományok azonnal nyilvánosan elérhetők, akkor ezek biztonsága kétes (a beérkező file-on legfeljebb azonnali automatikus vírusellenőrzés futtatható).

## 12. A World-Wide Web

A World-Wide Web megjelenésével az Internet átalakult, akadémiai hálózatból általános világhálózattá vált, melyen üzleti tranzakciók folynak, üzleti információk áramlanak. Hitelkártyaszámok haladhatnak titkosítatlanul, ellenőrizetlen lehet mind a fogadó, mind a küldő hitelessége. A Web üzleti alkalmazása töretlenül hódit, ezen akarnak vásárolni, kereskedni, pénzátutalást teljesíteni, bizalmas üzleti információkat lehívni az emberek.

Lássuk milyen kérdések, biztonsági problémák merülnek fel:

- felhasználó (kliens) azonosítás;
- szerver azonosítás;
- biztonságos út titkos információk számára (jelszavak, hitelkártya információk);
- információk hitelességének ellenőrzése és hitelesítés;
- kulcs menedzsment;
- lehallgatás elleni védelem;
- kompatibilitás (felülről kompatibilitás a régebbi kliens szoftverekkel és kompatibilitás a különböző védelmi és titkosítási módokat alkalmazó rendszerek között);
- a kliensek védelme;
- a szerverek támadás elleni védelme;
- a szerverek szándékos és akaratlan túlterhelése (pl. robotok 'támadásai');
- garantált szolgáltatás elérhetőség, sávszélesség, ismert korlátú válaszidők.

Itt több, egymást átfedő kérdéskört soroltunk fel: pl. a lehallgatás elleni védelem miatt fontos a biztonságos út biztosítása. A fentiek mellett nem elég a Web-szintű védelem: pl. hálózati fizetések esetén a biztonság függ attól, hogy a háttérben milyen pénztranszfer rendszer működik.

A Weben nemcsak dokumentumok, hanem programkódok és program információ is haladhat, mely a kliensen vagy szerveren alkalmazásokat indíthat el (helper alkalmazások, PostScript megjelenítés, Java scriptek stb.). Ez egy forrongásban lévő terület, még nem gyűlhetett össze elég tapasztalat. Itt valójában nem kész termékek, hanem köztes fejlesztések kerültek alkalmazásra.

A szerző jelenleg úgy látja, hogy a felmerülő problémákkal együtt azok megoldása, sőt a szabványosítás is lépést tart. A titkosság és hitelesítés kérdéseire napjaink megoldásai közül talán a Netscape Co. **Secure Socket Layer** (SSL) szabvány tervezete és implementációi *(http://www.netscape.com)* a legfontosabbak, de nem egyedülállóak. Alább pár szóban ismertetjük ezt és egy másik szabványjavaslatot a Secure-HTTP-t a példa és a fentiek szemléltetésének kedvéért.

Felhasználó azonosítást, jelszókat, csoport jelszókat, IP cím- és névazonosítást (letiltást vagy engedélyezést) számos HTTP szerver támogat (a legtöbb szerver még titkosítatlan jelszavakat használ).

A szervizek elérhetőségére a hierarchikus *cache*-rendszerek nyújthatnak hatékony megoldást (azonban itt újabb kérdések is felmerülnek, pl. a *cache*-beli információ érvényessége, naprakészsége).

A World-Wide Web technikája oly gyorsan fejlődik, hogy e füzetben talán kissé korai is lenne megoldásokat, javaslatokat ismertetni. Füzetünk egy későbbi változatában reméljük módunk lesz e fontos területet részletezni. További olvasmánynak javasoljuk még a később megjelenő két NIIF füzetet:

"**Böngészés a WWW-vel**" és "**Hogyan csináljunk saját WWW-t?**"

## Secure Hypertext Transfer Protocol (Secure-HTTP)

S-HTTP néven is ismert. *Draft* Internet szabvány, léteznek megvalósításai, gyakorlati alkalmazásai. Az S-HTTP nem önálló protokoll, hanem a szabványos HTTP kiterjesztése. Az S-HTTP képes az adatforgalom mindkét irányú titkosítását, digitális aláírás alkalmazását és hitelesítést biztosítani a kliens és szerver között. A választható titkosítási eljárásokra nem ad megkötést (támogatja a nyilvános kulcsok használatát is), megengedi nem-S-HTTP tudatú kliensek alkalmazását is (sőt kényesebb igényeknek is eleget tesz).

## Secure Socket Layer (SSL)

A Netscape által kifejlesztett és támogatott SSL nem a HTTP kiterjesztése, nem is kizárólag Web-specifikus, más Internet alkalmazásokhoz is használható (így az S-HTTP-vel is kompatibilis). Az SSL a HTTP-nél alacsonyabb szintű protokoll, biztonságos csatornát képes létrehozni két végrendszer között: *end-to-end* titkosítást, digitális aláírást, kliens és szerver azonosítást stb. támogat. Az SSL külön URL használatát követeli meg ún. biztonságos szerverek esetén (*'https://'* kezdetűt a *'http://'* helyett). A Netscape és számos más kliens program képes kezelni az SSL-t, s a kliens grafikus felülete jelzi, hogy biztonságos, vagy nem biztonságos szerverhez csatlakoztunk.

## 13. A dial-up kapcsolat

Napjainkban a *dial-up* kapcsolat mind az Internet használatában, mind a távmunkában jelentős szerephez jutott. A dial-up felhasználás problematikája sokban különbözik a helyi hálózatokról történő eléréstől. Itt a felhasználók általában egy kereskedelmi szolgáltatón keresztül érik el az Internetet, vagy munkahelyükre csatlakoznak modemen (esetleg terminál adapteren) keresztül.

Klasszikusan biztonsági megoldásként alkalmazták a **dial-back**-et, azaz a felhasználó **visszahívás**át. Ekkor a felhasználó bejelentkezik, majd bont a kapcsolat és a hívott gép visszahívja (esetleg egy másik vonalon) a felhasználót. Ezzel a felhasználó telefonszámának azonosítása megoldódott. Ma a visszahívás inkább a hívó pénztárcájának kímélése érdekében történik. A visszahívás sok visszaélésre ad alkalmat a nem rendeltetésnek megfelelő használat esetén (pl. a munkáltató számláján keresztül magán-internetezünk, faxolunk stb.). Megjegyezzük, hogy az ISDN sokkal több biztonsági szolgáltatást nyújt, mint az analóg vonal.

Bár kapcsolt telefonvonali hívásnál is lehet alkalmazni titkosított vagy egyszerhasználatos jelszavakat, vagy a vonal forgalmának titkosítását, de ez nem szokásos. Így dial-up jelszavaink titkosítatlanul haladnak az Internet szolgáltatókhoz vagy az egyéb online szolgáltatókhoz. Ez gyakorlatilag nem vált ki aggódást a felhasználókból. (Pillanatnyilag a dial-up Internet szolgáltatóknál a titkosítatlan jelszavak használata a szokásos).

A dial-up Internet szolgáltatók esetében érdemes tájékozódni, hogy milyen biztonsági politikát követ a szolgáltató, s milyen megoldások vehetők igénybe. Egyes szolgáltatók nyílt biztonsági politikát követnek, azaz biztonsági megoldásaik nyilvánosak, mások titkolódznak. A nem nyílt biztonsági politika semmiképpen nem tekinthető modernek, talán tisztességesnek sem.

## 14. Tűzfal

A tűzfal *(firewall)* találó elnevezés, a közönséges megfelelőjéhez hasonló szerepet tölt be, célja nem a támadás lehetőségének kiküszöbölése (a tűz megakadályozása), hanem akadályt állítani a támadás elé, a sikeres behatolás valószínűségének csökkentése (a tűz tovaterjedésének megakadályozása). Azaz: a tűzfal nem a védelem alapeszköze, inkább fontos kiegészítője.

Alkalmazásuk egyre inkább terjed. A routerek nagy része számos tűzfal funkciót képes ellátni. A tűzfal egyik típusa az ún. 'külső tűzfal' a teljes helyi hálózatot részben izolálja az Internettől, míg az ún. 'belső tűzfal' a helyi hálózat egy különösen védendő részét zárja el annak többi részétől (és így az Internettől is). A tűzfal használata titkos, érzékeny *(sensitive)* adatok védelme, vagy nagy üzembiztonságot kívánó hálózatok esetén elengedhetetlen.

Manapság, amikor cégek, intézmények nagy számban csatlakoztatják hálózataikat az Internetre, a tűzfalak - melyek védelmi falként funkcionálnak a saját hálózat és az Internet között - rendkívül fontossá váltak, használatuk igencsak terjed. Azonban nemcsak a hálózat üzemeltetőinek kell tudniuk a tűzfalakról, hanem a felhasználóknak is, akik tűzfal mögül érik el az Internetet ill. csatlakoznak rá, t.i. a tűzfal nem teljesen transzparens a felhasználók számára, azaz tisztában kell lenni a korlátozásokkal. Ezek a korlátozások helyről helyre változnak.

A tűzfal - hasonlóan a hétköznapi szerepéhez - akadályt jelent a helyi és a külső hálózat között, melyen bizonyos forgalom egyik vagy mindkét irányban nem mehet keresztül, ill. valamilyen további ellenőrzésen megy keresztül. Azaz a tűzfal bizonyos mértékig izolálja a belső hálózatot. Az itt megadott leírás a 'külső tűzfalra' *(external firewall)* vonatkozik, ugyanis használnak tűzfalat *(internal firewall)* a belső hálózatok szegmentálására, egyes védett részek izolálására is.

A tűzfal szerepét játszhatja egy intelligens router, megfelelő konfigurációjú Unix gép, vagy több is ezek közül. Internet tűzfalnak egy PC-n futó szoftver is kiválóan megfelelhet.

A tűzfal bizonyos protokollokat átenged (ún. 'biztonságos protokollok'), míg másokat nem (ismeretlen vagy ún. 'veszélyes protokollok', pl. tftp, r-protokollok). Bizonyos protokollokat nem enged be: pl. a *finger*-re válaszolhat, de nem a *finger*-rel kérdezett gép, hanem helyette maga a tűzfal. Más esetben (pl. *News*) magán a tűzfal gépen lehet elérni a *newsgroup*-okat, vagy más szolgáltatásokat.

A tűzfal egyes protokollokat csak egyik irányban engedhet át: pl. kifelé lehet *telnet*-ezni, befelé nem. Ez kellemetlen csalódást okozhat egy külföldre utazott alkalmazottnak, amikor azt veszi észre, hogy saját gépébe nem tud bejelentkezni, nem éri el leveleit, stb.

Más módon is védhet egy tűzfal, korlátozva bizonyos portok elérését, további azonosítókat, jelszavat kérhet, s még számtalan módon szűrheti az információt.

A tűzfalak rendszerint folyamatosan jegyzik a forgalom bizonyos adatait, a bejelentkező gépek, felhasználók azonosítóit, rendkívüli és kétes eseményeket, továbbá riasztásokat is adhatnak.

Fontos megjegyezni, hogy a tűzfalak megfelelő konfigurálása nehéz feladat, s a tűzfal - hasonlóan a valódi tűzfalhoz - nem biztosít tökéletes védelmet, de a 'tűz' továbbterjedését gátolja.

## 15. Egyfelhasználós rendszerek védelme

A legtöbb felhasználó PC-s DOS-t vagy MS Windows-t használ. Ezek egyfelhasználós rendszerek, eredendően legfeljebb helyi hálózati használatra tervezettek, ahol a hálózat legfontosabb feladata az állománymegosztás és a háttértárolás. Ma ilyen operációs rendszerek (és hasonlóan a Macintosh, Amiga stb. gépek alapértelmezésű operációs rendszerei) alatt teljes Internet kiszolgálót, FTP szervert stb. futtathatunk. Számos ilyen program konfigurálható úgy is (sőt alapértelmezésben ilyen vagy csak így futtatható), hogy pl. az FTP szerver futása alatt bárki bejelentkezhet a PC-nkre, s akár az egész állományunkat törölheti. A veszély ugyan kicsi, mert csekély a valószínűsége, hogy valaki a PC-nkre vadásszon a szerver futási ideje alatt, de fennáll. Emiatt ajánlatos az adott szoftver dokumentációját védelmi szempontból is áttekinteni, s ha ilyen téren a dokumentáció vagy a védelem hiányos, akkor más szoftver után érdemes nézni.

A mai egyfelhasználós rendszerek már igazából nem egyfelhasználósak, *peer to peer* kapcsolatot, állomány-kiszolgálást stb. biztosíthatunk rajtuk. Ezekre végül is a többfelhasználós rendszerekre mondottak irányadók, annak figyelembevételével, hogy lehetőségeink (kontroll, auditálás) korlátozottabbak. Az erőforrás megosztás terén is szűkek a kontroll lehetőségei (pl. az MS Windows *kooperatív multitasking*-ja miatt).

## 16. Speciális veszélyforrások, kérdések

Néhány nagyon gyakori, elterjedt biztonsági problémát külön is szeretnénk kiemelni, melyek bár némileg alkalmazás-specifikusak, de általánosan elterjedtek, s jellegüknél fogva állandó biztonsági problémák okozói.

### Az X Window

Az X Window a legelterjedtebb osztott grafikus (ikonos/ablakos) felhasználói felület (rendkívüli előnye, hogy platform-független). Alkalmazása esetén a felhasználó gépén fut egy ún. terminál (X) szerver, melyet alkalmazás-szerveren futó alkalmazások, mint kliensek szolgálnak ki. A X felület rendkívül rugalmas, könnyen kezelhető, hatékony és sokoldalú, de használata veszélyeket rejt, különösen, ha nincs megfelelően konfigurálva. Itt részletesen nem kívánjuk az X Window biztonsági kérdéseit tárgyalni, csak a biztonsági hiányosságra mutatunk példát:

Az ún. 'xhost +' parancs engedélyezi, hogy bármely hostról kliens csatlakozzon az X szerverünkhöz. Kevésbé veszélyes, ha tréfából kollégáink X ablakokat jelenítenek meg terminálunkon, de nyilvánvaló, hogy ennél több is megtehető. Egyébként az 'xhost +' parancs sokszor az X szerver alapértelmezésű beállítása.

Az X Window számos régebbi implementációja súlyos hibákat tartalmazott.

### Az 'r' parancsok

Az 'r' parancsok ('rlogin' és hasonlók) a Berkeley Unix-ból származnak, ma már szinte minden Unix rendszer és számos nem Unix alatti TCP/IP csomag részei. Az 'r' parancsok lehetővé tehetik egy adott hostra bizonyos hostokról (ún. biztonságosnak tekintett hostokról) felhasználói név vagy jelszó kérés nélküli csatlakozást. Így hostok láncolata jöhet létre, melybe bárhol behatolva a láncon végig lehet haladni.

### Az NFS

A Sun Microsystem által kifejlesztett TCP/IP feletti (heterogén) rendszerek közti transzparens file elérést biztosító **Network File System** (NFS) használata hasonló rendszereknél nagyságrendekkel elterjedtebb. Eredetileg Unix (SunOS) alá fejlesztették, de ma már mikroszámítógépes operációs rendszerektől a nagygépekig széles körben elérhető és használt. Az alapváltozat védelme gyenge (nem biztonsági hibákból miatt, hanem magából a konstrukcióból fakadóan: az NFS-t használó gépek kölcsönösen biztonságosnak tekintettek), illetéktelen hozzáféréstől távolról sem védtelen (számos újabb implementációja már védettebb, pl. az Sun Secure NFS-e).

A fő problémák mégsem a gyenge védelemből fakadnak, hanem a **rossz konfigurálás**ból. Az egyik leggyakoribb hiba: írásjogot megadni minden hostnak (a 'kiexportált filesystem'-re), mely nem szerencsés módon általában - szinte kivétel nélkül - az **alapértelmezés** (ez tekinthető úgy is, mint egyfajta biztonsági hiba). Lehetőleg a 'rw' (olvasás-írás) jogokat írjuk át 'ro'-ra ('read only'), és ha mégis írás jogot kell biztosítanunk, akkor korlátozzuk le a 'rw' elérést hostokra (sőt ennél többet is kellene tennünk ...).

Fontos megjegyeznünk, hogy az NFS-t számos más módon is lehet rosszul konfigurálni! - és sajnos ezekkel a lehetőségekkel gyakran 'élnek is' a (kevésbé képzett) rendszergazdák.

## Törlés, felülírás, csoportmunka

Az operációs rendszerek, adatbázis-kezelők, egyéb alkalmazások rendszerint lehetővé teszik az adatok, rekordok, file-ok stb. törlését, felülírását. Mivel folyamatos mentés ritkán oldható meg (pl. napi mentés van), ezért bizonyos helyreállításra, újrafeldolgozásra, azaz plusz munkára van szükség véletlen törlés vagy hiba által bekövetkezett adatvesztés esetén.

A véletlen törlés ellen védekezhetünk a file írásvédetté tételével, bár ekkor pont módosítani, dolgozni nem tudunk a file-on. Számos operációs rendszer biztosít lehetőséget a file-rendszerek egyes elemeinek visszaállítására, ilyen esetekben a file-ok lényegében csak törlésre jelölődnek ki, de fizikailag nem törlődnek. Azonban vannak esetek, amikor egy operációs rendszer nem így működik, éppen biztonsági okok miatt (a titkosság érdekében) azonnal töröl, más esetekben pedig felülírás következhet be. A felülírás esélye az idő múlásával növekszik. Bizonyos grafikus felhasználói felületek ill. operációs rendszerek vagy segédalkalmazások lehetővé teszik, hogy a törlendőket átmeneti tárolóba tegyük (pl. a Macintosh System 'kukásedényébe'), és onnan visszanyerhessük azokat. Más rendszerek biztosítják, hogy verziószámokkal mentsünk, vagy folyamatosan készítenek biztonsági másolatokat, esetleg pl. egy dokumentum vagy CAD rajz minden szerkesztési műveletét mentik, így a visszaállítás a szerkesztés minden fázisában lehetséges.

Alapjában véve itt minden egyszerű és világos. A helyzet akkor kezd bonyolódni, amikor csoportmunkát végzünk, ugyanazt a dokumentumot, adatbázist többen szerkeszthetik, módosíthatják, törölhetnek benne. Ez esetben körültekintőbben kell eljárni, már az alkalmazott eszközök (szoftver) megválasztásánál. **Egyfelhasználós szoftverek nem támogatják a csoportmunkát**, ilyenkor csoportmunkát (méghozzá jól) támogató szoftvereket kell alkalmazni. Emellett ki kell alakítani a csoportmunka rendjét. A csoportmunka esetén a dokumentumok különböző változatai jöhetnek létre, problémák adódhatnak, ha egyidejűleg többen szerkesztenek egy dokumentumot.

A csoportmunka szoftvereknek támogatnia kell:

- a finoman beállított jogosítványokat;
- a pontos könyvelést (ki, mit, mikor végzett, módosított);
- az integritást és hitelességet általában.

Itt a szoftver gondos kiválasztására hívjuk fel még egyszer a figyelmet. A szoftver jó megválasztása mellett persze annak ésszerű használata is elengedhetetlen.

Bár már az előző fejezetekben említettük, itt megismételjük, hogy minden felhasználó egyedi azonosítóval férjen hozzá minden rendszerhez! Ne alkalmazzunk csoport accountokat, nyilvános accountokat és jelszavakat!

### Másolás védelem

A másolás védelem a szoftver gyártók klasszikus eszköze az illegális (pontosabban az ő érdekeiket sértő) másolás ellen. Vannak mind szoftveres, mind hardveres (és hálózati) eszközei. Itt a védelem feltörhetetlensége és a védelem által okozott esetleges károk, kellemetlenségek jelentik a biztonsági kérdéseket. Lehetőség van a hálózatba kötött gépünk szoftvereibe gyárilag beépíteni olyan programrészeket, melyek pl. az Interneten keresztül - akár a tudtunk nélkül - értesítik a gyártót az illegális szoftverhasználatról. Egyes esetekben a szoftvert hálózaton vagy modemes telefonkapcsolaton keresztül (első) használat előtt regisztráltatni kell (e nélkül nem indul vagy nem működik megfelelően).

A másolás elleni védelem érzékenyen jelentkezik WWW oldalak (és más online publikációk) esetében, amikor a szerző megtekinthetővé akarja tenni a dokumentumát, de nem másolhatóvá. Megjelentek e téren az első termékek, de tökéletes megoldás nemigen várható, hiszen, ha adatokat megtekinthetünk, akkor le is másolhatjuk őket (bár érhetnek meglepetések). Mindenesetre a másolás, nyomtatás útjába akadályok gördíthetők. A kérdés fontos, időszerű, de nem tudjuk mélyebben tárgyalni a kérdéskört, mivel még gyerekcipőben járnak a megoldások (bár egyszerű trükkök ismeretesek, melyekkel az átlagfelhasználó eszén túl lehet járni).

### Kiszolgáltatottság

Köd veszi körül, hogy a rendszergazdákat, hálózatmenedzsereket stb. milyen felelősség terheli és milyen hatalom van a kezükben. Végrendszerek esetében ez jobban átlátható, de a kommunikáció útjai kifürkészhetetlenebbek. A rendszerek nagy részénél (pl. az Internet, a legtöbb helyi hálózat) elvben minden adatforgalmat figyelhetnek, manipulálhatnak, egyedül önnön becsületük a korlát. Természetesen ez így nincs jól. A megoldás kulcsa azonban elsősorban nem a technikán, hanem az informatikai menedzsment - vezetés - és a helyi informatika hármasának viszonyában van. S persze az általunk elért külső hálózatok (pl. IP szolgáltatónk) menedzsmentje is alapvető biztonsági tényező. Érdemes felmérni, hogy kinek milyen manipulatív lehetőségei vannak egy hálózatos rendszeren (a biztonsági politika kidolgozásának ez része). E kérdések ma Magyarországon meglehetősen időszerűek: nyugati technikát használunk alacsonyabb informatikai kultúrával.

## 17. Hibák, történetek, érdekességek

Ebben a fejezetben részben ismétlésként, részben hiánypótlásként rámutatunk néhány fontosabb vagy érdekes hibára, veszélyre. Megtörtént esetek ihlették egyikmásik bekezdést.

### Alapértelmezésű jelszó

Korábban számos operációs rendszert alapértelmezés szerint installálva bizonyos (fiktív) felhasználói nevek alapértelmezésű jelszóval jöttek létre. Ma is számos alkalmazásnál felbukkannak az alapértelmezésű jelszavak, az ilyeneket változatlanul hagyva rendszerünket veszélynek tehetjük ki.

### 'C2 security'

Számítógép-biztonság kapcsán gyakran hangzik el a misztikus 'C2' kifejezés. Misztikus, mert félreértik, helytelenül, de legalábbis pongyolán használják és köd lengi körül (természetesen nem a biztonsági szakemberekre gondoltunk). Valójában olvasóinknak elég azt megjegyezni, hogy ha C2-t emlegetnek, akkor tudják, hogy számukra érdektelen dologról van szó. Mi is az a C2? Az amerikai hadügyminisztérium egy (1985-ös) szabványa automatikus adatfeldolgozó rendszerek biztonsági kérdéseire létrehozott egy szabványt, népszerű nevén az **Orange Book**-ot. Ez osztályokba sorolta a rendszereket biztonsági kritérium szerint, s egy ilyen osztály a C2. Csak C2 osztályba sorolt rendszert szabad az Egyesült Államokban bizonyos állami hivatalokban adott feladatokra alkalmazni. Noha a szabvány tanulságos lehet egy szakembernek, nemigen lehet módunk eldönteni, hogy egy rendszer eleget tesz-e a C2 követelménynek, vagy sem. Az a gyakran alkalmazott reklám, hogy X.Y. operációs rendszer eleget tesz a C2 követelményeknek, értelmetlen az Orange Book szerinti nézőpontból. Kellően rosszul installálva, nem biztonságos hálózatba kötve egy rendszer nemhogy C2, de semmilyen követelménynek nem tesz eleget (ill. a bizonytalan rendszer követelményének eleget tesz). Még egy gondolat: az Orange Book-nak egész sor kiegészítése született (Rainbow Series), ezek egyes környezetekre éppen olyan jelentősek, mint az alapmű (pl. hálózatot explicite nem említ az Orange Book, ezt egy másik színes könyv tárgyalja).

### Dohányzás

A dohányzás legalább annyira káros számítógépes rendszereinkre, mint az emberekre. A hamu eltömi a hűtőberendezéseket, lerakódása zavarja a hőleadást. A dohányfüst korróziós hatása is jelentős, lerakódása kisüléseket okozhat a mikroáramkörökön. Kívül-belül összemocskolja a berendezéseket (dohányzás miatt elpiszkolódott berendezésre nem vonatkozik garancia). Számos speciális kár okozásáért is felelős vagy felelős lehet. Egyértelműen kimutatott, hogy sok hardver (merevlemezes egységek, hajlékonylemezes meghajtók, egerek stb.) élettartamát

lényegesen (10-30 %-kal) csökkenti. Nehéz megérteni, hogy egyes munkahelyek még csak nem is korlátozzák vagy szankcionálják a dohányzást.

### Domain Name System

Ha DNS szerverünk először egy másik géphez irányítja a levelet (pontosabban a másik gép preferáltabb az MX bejegyzés szerint, azaz kisebb a preferencia indexe), csak utána a rendeltetési helyhez, a két gép ráadásul egy hálózaton helyezkedik el, valamint teljes Internet eléréssel és *mail transport agent*-tel rendelkezik, ez ekkor már gyanús: valami különleges ok áll fenn, esetleg tévedés történt, netalán csak leveleinket akarják tanulmányozni.

### Elektronikus levélcímünk változása

Levélcím változás esetén, ha lehet azonnal ne szüntessük/szüntettessük meg régi címünket, onnan átirányítást biztosítsunk vagy kérjünk. Rengeteg levél megy ismert, de nem működő címekre, ahol gyűlnek az olvasatlan levelek, bosszankodnak a feladók. Közismert példa az Ella rendszer (ráadásul itt sok felhasználó soha sem tudta, hogy ő felhasználó).

### Elfelejtett rendszeradminisztrátori jelszó

A rendszeradminisztrátori jelszó sem elfelejthetetlen, valamint más okokból is elveszhet. Bár az operációs rendszerek jelentős része a jelszó visszaállítását nem teszi lehetővé, egy kerülő út áll rendelkezésre a *superuser* jelszó megváltoztatására. Számos Unix, a Novell NetWare 2.x és 3.x esetén ez rutinfeladat (elég csak a géphez vagy a konzolhoz hozzáférnünk). Azonban több újabb operációs rendszer már védettebb (pl. a NetWare 4.x), ezeknél súlyos baj lehet a rendszeradminisztrátori jelszó elvesztése.

### Írható távoli file-rendszer vagy annak írható könyvtára

A veszélyek sora szemben a praktikummal. Ne engedjünk meg véletlenül több jogot az olvasásnál! Ne engedjünk nyilvános írásjogot! Ne azt határozzuk meg, hogy ki, mihez nem férhet hozzá, hanem adjuk meg a szükséges jogokat, és azon kívül tiltsunk meg minden mást! Többfelhasználós rendszerek lokális file-rendszerein is elkél az óvatosság. *(Lásd még az előző fejezetben : "Az NFS").*

### A jelszógyűjtés egy sajátos módja

Ha egy kellően érdekes, vonzó szolgáltatást hozunk létre saját rendszerünkön, ami csak a felhasználó által szabadon, de kötelezően választandó jelszóval érhető el, akkor a választott jelszavakat összegyűjthetjük. Mivel a felhasználók részben megszokott jelszavaikat használják, így ezekkel jó eséllyel kezdhetjük meg behatolásunkat más rendszerekbe. Konklúzió: nem szabad különböző (logikailag nem összefüggő) rendszereken azonos jelszavakat használni!

### Jelszó nélküli accountok

A tapasztalat azt mutatja, hogy a felhasználók 10-30 %-a - ha teheti - jelszó nélkül használja accountját, teljes jogot engedve másoknak levelezéséhez, adataihoz. Ahol a személyes adatok kevésbé értékesek, ott az arány még magasabb. Sokfelhasználós rendszerek esetén a helyes jelszófelhasználás gyakran csak retorziókkal érhető el.

### Hálózati erőforrások indokolatlan terhelése

Ez inkább etikai, mintsem biztonsági kérdés, azonban a szolgáltatások elérhetetlenségét, használhatatlanságát okozhatja, így nem lehet csak etikai kérdésként hozzáállni. Bár követni, illetve (főleg szúrópróbaszerűen) ellenőrizni lehet, hogy a felhasználók mit csinálnak, ez a személyiségi jogokat sértheti és etikai szempontból sem elfogadható. Így csak a tájékoztatás, oktatás, nevelés és propaganda segít.

### A hálózati dokumentáció hiányossága

Egy hálózati hiba (pl. vezeték sérülés) megtalálása rendkívüli feladat lehet, ha nem tudjuk, hogy merre haladnak a vezetékek.

### Hardver kulcs

A hardver kulcs általában másolás, ritkábban hozzáférés elleni védelmet szolgál. Egy szoftver felhasználójának ritkán érdeke az ilyen másolásvédelem, emellett ez kellemetlenségekhez vezethet (a hardver kulcs zavarhatja a normális működést vagy üzemeltetést, a kulcsok elveszthetők, ellophatók, megsérülhetnek). Érdemes tudni, hogy számos hardver kulcsos terméknek van kulcs nélkül működő változata is, vagy forgalomban van olyan szoftver, amely inaktiválja a kulcsot.

### Közös jelszó, jelszó átadása

Azért szokás ilyen eszközökhöz folyamodni, mert valamely adatot szeretne valaki mással megosztani. Ehhez a megoldáshoz nyilván azért fordul a felhasználó, mert más, jobb utat nem ismer. Pedig van! File/könyvtár hozzáférési jogok megadása, levélátirányítás stb. Csak egy kis fáradságot kell venni rendszereink megismeréséhez.

### Levélben kért jelszó

Sok rendszergazda hajlandó (elektronikus) levél, telefon/fax stb. kérésre megváltoztatni egy felhasználó jelszavát. Vagy letörli a jelszót (az account jelszó nélkül marad), vagy titkosítatlanul elküldi. Természetesen privilegizált account esetében ilyet senki nem tesz. Ez az utóbbi időkig talán rendjén is volt, de nem lehet így a hálózati vásárlások korában.

### Maximált file-méret

Számos rendszerben (a legtöbb Unix alatt) szokás a maximális file-méret alkalmazása. Az aktuális korlát ismerete hiányában a felhasználó többször nekirugaszkodik letölteni egy 120 MB-os file-t, s 100 MB-nál rendszeresen elakad. Ezzel alapos nem kívánatos hálózati forgalmat generál.

### Mobil telefon

A füzet egyik szerzőjével a füzet írása közben fordult elő, hogy hajlékonylemezen akart átadni egy kollégájának egy fontos dokumentumot. A lemezt zsebre vágta - éppen a mobiltelefonja mellé. Egy hívás, s az adott file lemezhiba miatt részben olvashatatlanná vált.

### Quoták hiánya

Az elérhető maximális tárterületekre nézve számos rendszernél nem alkalmaznak korlátozásokat, vagy a rendszer ideiglenes felhasználásra tárterületet biztosít. Ekkor pl. egy felhasználó által kiadott Unix parancs, 'cat * > valami' pillanatok alatt betöltheti a rendszer teljes kapacitását.

### RAID technológia

A technológia eredetileg olcsó, relatíve kis kapacitású diszkek együttes használatát jelentette a teljesítmény és a megbízhatóság (hibatűrés) fokozására. Az idevonatkozó szabvány RAID 1, 2, ... 5 kategóriát (ma 7-ig, ill. egyes kombinációk definiáltak 10, 53, stb. néven is) határoz meg (a szintek más-más teljesítményt és hibatűrést biztosítanak). A diszkekre/ről egyszerre történhet írás, olvasás, ellenőrző összegek és/vagy redundáns adatfelvitel révén. A technológia általánosan alkalmazott szerverek esetében, de munkaállomások és PC-k esetében is (nagygépeknél más módszereket találunk). Rendszerint speciális RAID kontroller kártyát használnak, ritkábban tisztán szoftveres megoldást. Az SCSI diszkek használata az általános, de IDE RAID csatolók is forgalomban vannak. Egyes esetekben a (meghibásodott) diszkek leállás nélkül cserélhetők *(hotplugable disks)*. A módszer ma már sok esetben azonos vagy nagyobb hibatűrés és teljesítmény mellett is olcsóbb, mint a diszktükrözés (azaz minden adat két független diszkre történő írása).

### Rendszeradminisztrátori account

A rendszeradminisztrátori (supervisori) és más privilégizált accountot csak akkor és arra használjuk, amit máshogy nem lehet megoldani, és csak arra az időre jelentkezzünk be így, amíg az adott feladatot elvégezzük. Nyilvánosan elérhető gépről ne használjunk ilyen accountokat (sőt hálózatról sem). Az előbbiek igazak

nemcsak az ilyen accountok használatára, hanem minden privilegizált hozzáférésre (pl. a Unix 'su' parancs használatára). Ne írjunk és fogadjunk levelet privilegizált accountról/ra (használjunk ún. *mail alias*-t), s ez érvényes talk, IRC és egyéb konferencia programokra, s természetesen minden játékprogramra is.

### A rendszer erőforrásainak terhelése

Önön szórakoztatásunkra elindítunk néhány dekoratív X alkalmazást ('X szemet') és a rendszer erőforrásainak nagy részét ezzel lekötöttük. Majd kiadunk egy keresést (*find* parancsot Unix alatt), s a rendszer majdhogynem megáll. A példákat sorolhatnánk.

### Reset gomb

Többfelhasználós rendszert nyugodt szívvel kapcsolhat ki vagy indíthat újra egy átlagfelhasználó, ha lefagy a terminálja. Persze ezt nem teszi, ha erre nincs módja, vagy csak különös nehézségek árán kivitelezhető. Egyesek nem tudnak ellenállni a szünetmentes tápegység kikapcsológombjának. Az igazi megoldás a fizikai védelem - eltávolítani, beragasztani minden nyomógombot :-). Persze elárulhatjuk a felhasználóknak az alternatív lehetőségeket is (pl. keresse a rendszergazdát, vagy hogy mely billentyűkombinációval próbálkozzon ilyenkor).

### Rossz jelszavak

A felhasználók előszeretettel alkalmazzák (ha csak tehetik) az alábbi típusú jelszavakat:

- saját login név, név, becenév, családtag, barátnő neve;
- saját telefonszám, gépkocsi rendszám;
- munkakörre, munkahelyre, hobbira vonatkozó szó.

Vannak népszerű jelszavak. Egyes felmérések szerint kevesebb mint ezer jelszó lefedi a világon számítógép eléréshez használt jelszavak több mint felét.

### Single user üzemmód, magára hagyott szerver

Mint fent említettük az elveszett jelszó ürügyén: a magára hagyott gépek jelszavai nagyon sok esetben feltörhetők (a PC-k *setup* jelszava általában - közismert módon - feltörhető, sok Unix esetében az ún. *single user* mód nem kellően védett). Itt adott esetben csak az operációs rendszer upgrade-je, cseréje, a hardver le- vagy elzárása esetleg cseréje szolgáltathat megoldást - vagy a biztonsági rés tudatával kell együtt élnünk.

### Szoftver upgrade

Rengeteg hiba forrása mind az *upgrade*, mind annak hiánya. Példák az *upgrade* lehetséges problémáiból (nem csak operációs rendszerre, de elsősorban arra gondolunk):

- számos bevált alkalmazásunk nem működik;
- interoperábilitási, kompatibilitási problémák bukkanhatnak fel;
- meg kell tanulnunk használni az új rendszert;
- ismeretlen jelenségek léphetnek fel, hibák bukkanhatnak elő;
- mentésünk visszaállításánál problémák léphetnek fel.

Az operációs rendszerek és az összetettebb alkalmazások biztonsági szempontból sohasem tökéletesek. Számos hibát észlelnek a fejlesztők, melyekre vagy javításokat *(patch)* adnak ki, vagy az újabb változatokból már kiiktatják a hibákat. Az újabb változatok is tartalmazhatnak persze biztonsági lyukakat, de ezek még nem kerültek napvilágra, így a támadók is kisebb eséllyel használják ki ezeket.

### Superuser account megszerzése

Az illetéktelen machinációk elsődleges célja a *superuser* jogosítvány megszerzése. Innen már minden elérhető.

### Szalámi technika

Egy pénzügyi program kerekítési szabályainak s hasonlóknak apró megváltoztatása, majd a töredékösszegek folyamatos átirányítása, állandó bevételhez juttathatja a címzettet. Klasszikus eljárás a pénzforgalom megcsapolására.

### A visszaállítás nehézségei

Gyakori eset, hogy a mentés akkurátus pontossággal végrehajtott, szépben őrzik a mentést, ... Azonban amikor (akár évek múltával) először következik be adatvesztés, a visszaállítás nem sikerül. Ritka, hogy ilyen esetben a visszaállítást valahogy ne lehetne végül is megoldani, de megoldhatatlan esetekre is számos példa volt.

## 18. Az Internet biztonságáról, speciális biztonsági kérdéseiről

Az Internet központi menedzsment nélküli heterogén hálózat. Elvben bárki vagy bármely szervezet csatlakozhat hozzá. Nincs az egész Internetre nézve kötelező elv, felhasználási és biztonsági politika. Az Internet és számos még lazább, szabadabb szervezetű hálózat (UUCP, Fidonet stb.) között átjárók vannak. Az Internethez szervezetek, cégek, magánszemélyek csatlakoznak, nagy számú szabadon elérhető dokumentumot, programot, adatot helyeznek el rajta.

Azonban az Internet nem menedzseletlen, valamint korlátozott központi adminisztráció működik: menedzselt hálózatok, menedzselt elérési pontok, egymással együttműködő menedzsmentek, szervezetek vannak. Egyes részein többé-kevésbé szigorú felhasználási politika van érvényben, s vannak általánosan elfogadott normák, szokások.

Cégek csatlakozásánál a legelőször felmerülő kérdések egyike a biztonság. Azonban a nyilvánvaló előnyökkel szemben a biztonsági okokból való elzárkózásnak nemigen lehet realitása. Egyrészt lehet az Internet felett virtuális privát hálózatot, vagy az Internet elérést mint multiprotokoll hálózat részét biztosítani, ill. magánhálózaton az Internet elérést virtuális hálózatként biztosítani. A biztonság bár fontos, az aktuális és potenciális Internet forgalom igen kis része követelne nagyobb biztonságot.

Az Internet sajátos jelenség a számítógép-biztonság számára, azonban nem rendelkezik egyedi, máshol nem fellelhető problémákkal. A tipikus gondok:

- nagy számú, egyfelhasználós PC csatlakozása;
- növekvő számú dial-up kapcsolat;
- gyenge védelemmel és laza menedzsment alatt működő szerverek;
- az általánosan terjedő lehallgatás.

A problémák egy része ún. *'a végfelhasználó vessen magára, ha'* jellegű, de az ilyenek jelenthetnek szélesebb körű veszélyt is. Pl. nem biztonságos node-ok 'r' láncolata *(lásd az előző fejezetet)*, ellenőrizetlen szoftverek terjesztése.

A problémák másik része a kialakulatlan üzleti tranzakció-mechanizmusokra vezethető vissza, bár itt nagyon gyors a fejlődés.

Egy sajátos gond - melynek jelentőségét messze eltúlozzák -, az ún. *unreliable tranzakciók*, azaz nem garantáltan eredményes, nem garantáltan nyugtázott, nem garantált idejű tranzakciók. A túlzás abban van, hogy az Internet alternatívák sem mindig teljesítik az igényeket sokkal jobban. Egy tőről fakadó probléma az elérhetőség garantálása: a garantált válaszidők, a sávszélesség, a rendelkezésre állás biztosítása (*availability, denial of service*).

Egy másik sajátosság, hogy az Internet forgalma monitorozható, nincs mód a *packet header* információk titkosítására. Így nyomonkövethetők az adott helyen áthaladó hálózati csomagok: melyik host mely hosttal állt kapcsolatban? Más

módon, de a levelezés is részben figyelhető: ki, mikor, kivel levelezett? Bár az üzenetek és csomagok tartalma titkosítható, jelentős információszivárgás van e tekintetben. Ez alapvetően zavarja a magán és az üzleti élet titkosságát, sérthetők személyes szabadságjogok és üzleti titkok (az előzőekre az angol a *'privacy'* kifejezést alkalmazza, megfelelő magyar szó nem ismeretes). Megállapítható ill. valószínűsíthető, hogy pl. ki, milyen hálózati boltokkal lépett kapcsolatba, milyen hálózati magazinokat olvasott stb. Ma még e kérdésekre nincs gyakorlati megoldás (az Internet hálózati protokolljának, az IP jelen verziójának felváltása szükséges).

Mondják, hogy az Interneten nincs mód arra, hogy választ kapjunk levelünk megérkezésére. Ez így nem igaz, bár vannak korlátok. Ellenben más hálózaton esetleg arra sincs mód, hogy a potenciális címzettnek e-mail-t küldjünk - ugyanis az adott hálózaton nincs az illetőnek címe.

Az Interneten több igen gyenge pont van, ilyenek a névszervizek, a route-olás és a menedzsment, az utóbbi kettő technikailag túlmegy az átlag felhasználó érdeklődésén, de a névszervizeket nem hagyhatjuk szó nélkül. Az Internet két leghasználatosabb névszerviz szolgáltatása a Domain Name Service (DNS) és az X.500. Az X.500 meglehetősen erős biztonsági elvárásoknak is eleget tesz, de a DNS nem. Míg az X.500 nem kritikus szerviz az Interneten (más hálózaton gyakran az), addig a DNS igen. E füzetben nem foglalkozhatunk a DNS strukturális problematikájával. Míg a route-olás problémái elsősorban a szerverek elérhetetlenségében jelentkeznek a DNS-é nemcsak abban. A DNS-sel könnyen visszaélhet üzemeltetője: levelezésünket megfigyelheti, leveleinket elfoghatja, illetéktelen helyre átirányíthatja (bár ezt gyakorlatilag a levelezőrendszerek üzemeltetői is megtehetik, nagyipari méretben a DNS-t elkonfigurálva lehet a levelezést figyelni). A DNS egy jó példa arra, hogy az Interneten a titkosság *(privacy)* mennyire függ a rendszer- és hálózatmenedzserektől (ill. elvben e menedzserek tevékenységének ellenőrzésétől).

Az új Internet szabványok a biztonság minden terén kielégítővé teszik az Internetet - sajnos az implementációk még nem érhetők el a gyakorlatban. Új szabványok vannak az Internet alsó szintjének (az IP szintnek) biztonságossá tételére, s új ajánlások, javaslatok, részben szabványok a magasabb szintekre.

Az Internet speciális biztonsági problematikája kevésbé érinti a felhasználókat, mint a hálózati menedzsereket és rendszergazdákat. A problémák elenyészően kis része fakad magából az Internet biztonsági gyengeségeiből, zömük a felhasználók tudatlanságából, elemi szinten elkövetett hanyagságaiból származik. A nem reális üzenettovábbítás nagy része menedzsmentbeli hiba.

Már korábban is mondtuk, hogy az Internet globális biztonsága lépést tartott és tart az igényekkel; sok mindent nem teljesít, de a felhasználás céljai és a biztonság kellő arányban állt és áll. Manapság viszont a felhasználás új területeire tevődik a hangsúly. Mindazonáltal nem hiszem, hogy az Internet fejlődésének biztonsági problémák gátat vethetnének. Az Internet fejlődése biztonsági szempontból a motorizációhoz hasonlítható: a balesetek ellenére nem fogunk lemondani sem a motorizáció, sem az Internet áldásairól.

## 19. Az egészség és a környezet védelme

A fejlett világban egyre nagyobb figyelmet fordítnak a környezet és egészség védelmére, energiatakarékos megoldásokra. Nálunk sajnos nem ez a helyzet.

Számítógépes környezetben a legveszélyesebb egészségkárosító hatások az alábbiakból fakadnak:

- a nem ergonomikus környezet, a rossz testtartás;
- a rossz monitorok, a megfelelő monitorszűrők hiánya, ezek nem megfelelő használata (lásd a használati utasításokat);
- a nem ergonomikus billentyűzet és egér (ez csak az igen sokat gépelők számára jelent veszélyt, de náluk nem lebecsülendőt);
- a zaj;
- a légkondícionálók, a huzat stb. szintén sok bajnak forrásai.

Nyomtatókazettákat, festékpatronokat, elemeket, áramszolgáltató telepeket, monitorokat nem szabad szemétbe dobni. Ezek egy része újrahasznosítható vagy csak speciális módon tehető ártalmatlanná; összegyűjtésük szakszervizek feladata lenne. Nagyobb munkahelyeken a gyűjtés központilag oldandó meg (hasonlóan a többi speciális/veszélyes hulladékhoz).

Fontos megemlítünk, hogy mind a számítógépes berendezések, mind a hálózatok elektromágneses zajforrások. Beszerzésükkor, telepítésükkor erre figyelemmel kell lennünk.

## 20. Jogi és etikai kérdések

A biztonság számos ponton kapcsolódik a joghoz és az etikához: gondatlanság, szándékos rongálás, illetéktelen elérés, számítógépes bűnözés, elektronikus adatcsere, aláírás hitelessége, szerzői érdekek stb. Néhány gondolat, megjegyzés:

1. Általában nem igaz, hogy ne lenne - a magyar jog szerint - büntetőjogi felelősség és szankcionálási lehetőség a számítógépes visszaélések, illetéktelen behatolás, vírus terjesztés és más hasonló cselekedetek ellen. Az más kérdés, hogyha a felelősségrevonás elmarad.

2. A szerzői jogvédelem területén más hangzik el az illetékes hatóságok, hivatalok (pl. Szerzői Jogvédő Hivatal) és érdekvédelmi szervezetek részéről (pl. BSA), mint ami a jogszabályokban áll. Azt lehet mondani, hogy a jog és a gyakorlat nincs összhangban. Itt inkább az etikára kell hagyatkoznunk, mint a jogra, valamint más fejlett országok jogi szokásait követni. (A magyar szerzői jogot nem könnyű megsérteni, azonban a szerzői érdekeket igen - e füzet szerzői csak elvétve találkoztak jogsértéssel).

3. Számos érdeksértés fog bekövetkezni a viszonylag ellenőrizetlen média, az Internet jóvoltából. Látnunk kell azonban, hogy a jelenségek alapvetően nem térnek el más médiában (pl. a sajtóban) megszokottaktól. Számos kérdés jogilag szabályozatlan, de talán nem a jogi szabályozásnak kell élen járni. Érdemes megjegyezni, hogy az Internet nemzetközi hálózat, melyre az USA-nak alapvető befolyása van.

4. Megjegyezzük, hogy az Egyesült Államok export szabályozása nagyban gátolja a titkosítási eljárások és az ezeket alkalmazó hardver és szoftver nemzetközi elterjedését, exportját.

5. A digitális aláírás sokkal elfogadhatóbb, mint azt banki, vállalati és államigazgatási szakemberek általában gondolják. A terjedését azonban tévhitek is gátolják.

6. A felhasználási és biztonsági politikák hiányoznak, vagy nincsenek, vagy nem nyilvánosak (egy kirívó eset: a HBONE).

7. A felhasználási politikákban vagy azok mellett célszerű 'etikai szabályzatokat' is megfogalmazni és közzétenni.

8. A hálózati etikett (bár ilyen nem igazán létezik, hanem vannak illemszabályok elektronikus fórumok használatára és üzemeltetésére, Web publikálásra, 'ftp-zésre', elektronikus levelezésre stb.) nálunk még nem közismert. Az Internet vagy az elektronikus levelezés használata nyilván megelőzi a rájuk vonatkozó etikai normák megismerésesét. Az oktatás, tájékoztatás alapvető és állandó feladat.

9. Legyünk toleránsak, még a normák megszegőivel is! Legyünk óvatosak, ne hozzunk elhamarkodott ítéleteket! A normák megszegőit érdemes figyelmeztetni, de ha van erre illetékes személy (az illetékes postamester, hálózatgazda) akkor bízzuk arra. A figyelmeztetés a helyes út: ez jobb lehetőségek meg/bemutatásából álljon.

10. Az erőforrások illegális használata leginkább fiatalokra jellemző, az Internet betörési kísérleteinek nagy részét egyetemisták követik el. Úgy érzem, hogy a sértettek, az adott rendszerek üzemeltetőinek felelőssége ilyen esetekben nagyobb, mint a játékból/tudásvágyból próbálkozóké.

11. Mindig nyílt biztonsági politikát folytassunk! Ne kezeljünk titkosan semmit, ami valójában nem titkos, személyiségi jogokat nem sért. Az oktatásban se titkoljuk el a rendszerek gyengeségeit, az ismert biztonsági lyukakat. A lyukakat felszámolni kell, nem eltitkolni.

12. A biztonsági eseményekről mindig értesítsük az illetékeseket (sajnos ez - bár kivételesen - sértődésekhez vezethet).

13. A rosszul szervezett menedzsment, a kellő szabályozás hiánya az illetékességek terén állandó problémák forrása lehet. A célok meghatározásánál és a menedzsment kereteinél kell kezdeni minden szabályozást. Minden szempontból jól felépített rendszer jó menedzsment mellett minimálisra csökkenti a problémák számát.

14. Az egészség és a környezet védelmében is fontos feladatok vannak. Itt kiemelkedő hiányosságok tapasztalhatók.

## További segítség és irodalom

**Cliff Stoll: The Cuckoo's Egg**
Pocket Books
New York, 1990
ISBN 0-671-72688-9

Egy híres, megtörtént betöréssorozat irodalmi feldolgozása. Megjelenésekor az USA-ban bestseller volt. Regény létére tanulságos olvasmány mindenki számára, felér egy bevezető tankönyvvel.

**Deborah Russell, G. T. Gangemi Sr.: Computer Security Basics**
O'Reilly & Associates, Inc.
Sebastopol, CA, 1991
ISBN 0-937175-71-4

Kiváló alapkönyv. Széles áttekintést ad, s nem mélyül el a részletekben. A biztonsági kérdésekkel foglalkozóknak, rendszergazdáknak olvasniuk kell. A könyv nem foglalkozik platform- ill. operációs rendszer-specifikus dolgokkal.

**Peter J. Denning: Computer Under Attack - Intruders, Worms, and Viruses**
Addison-Wesley
NewYork, 1990
ISBN 0-201-53067-8

Biztonsági kérdések történeti áttekintéséhez, hátteréhez egy kedves, viszonylag könnyed olvasmány. Szabadidő olvasmánynak ajánljuk.

**Simson Garfinkel, Gene Spafford: Practical Unix Security**
O'Reilly & Associates, Inc.
Sebastopol, CA, 1993
ISBN 0-937175-72-2

Az egyik legjobb, a Unix biztonság alapjaival foglalkozó könyv. Kezdő Unixos rendszergazdák alapolvasmánya, de gyakorló Unix felhasználók és programozók szintén haszonnal forgathatják.

**Andrew S. Tannenbaum: Számítógéphálózatok**
Novotrade Kiadó - Prentice Hall, 1992
ISBN 963-585-162-6

Klasszikus tankönyv a számítógép-hálózatokról. 8. fejezetében (581-610. old.) részletesen ismerteti a kriptográfia alapjait, beleértve a digitális aláírást is. Sajnos a könyv eredetije 1989-ben jelent meg. Noha már sok újdonság jelent meg azóta, az alapok nemigen változtak.

**Peter Wayner: Digital Cash - Commerce on the Net**
AP Pofessional, 1995
ISBN 0-12-738763-3

Bár füzetünk nem az üzleti világ számára íródott, ma már senki sem mehet el a hálózat, az Internet üzleti alkalmazásai mellett. Az egyik legfontosabb terület az elektronikus pénz és fizetés *(digital cash)*. E könyv ezzel foglalkozik, kicsit több, mint az átlagolvasó minimum igénye, de közérthetően fogalmaz és jól fedi le a témát, kellemes olvasmány. Sajnos naprakész könyvet a téma fejlődésére tekintettel lehetetlen írni, de a leírtak nagy része ettől függetlenül a jövőben is alkalmazható lesz.

**Computer Security - Virus Highlights Need for Improved Internet Management GAO report, 1989 (GAO/IMTEC-89-57)**

Az US General Accounting Office első Interneten is elérhető jelentése, mely részletesen tárgyalja az Internet Worm történetét, technikai részleteit. Mindenkinek ajánljuk.

**R. Pethia S. Crocker and B. Fraser: Guidelines for the Secure Operation of the Internet**
RFC 1281, 1991

Néhány oldalas összefoglaló, mely ismerteti a legfontosabb vezérfonalait az Internet biztonságos használatának. Minden Internet felhasználónak és szerver üzemeltetőnek szól.

Biztonsági szempontból fontos FTP/Gopher/WWW helyek, online elérhető dokumentumok és szoftverek, levelezési listák és newsgroupok URL-jeiről részletes listát szándékosan nem akarunk itt megadni, hiszen a nyomdai átfutás ideje alatt e téren túl sok minden változhat, de füzetünk HTML változatában ez elérhető lesz. Néhány fontosabb URL-t azonban mindenképpen meg kell adnunk (ezek alatt, vagy innen induló linken keresztül szinte minden fontos biztonsági helyet elérünk az Interneten):

*http://www.austria.eu.net/www-security-faq.html*
(WWW biztonság);

*http://nsi.org/newstuff.html*
(biztonsági kérdések, aktualitás, hírek - nemcsak számítógép-biztonság);

*ftp://infor.cert.org/pub/cert*
(aktuális kérdések);

*http://ausg.dartmounth.edu/security.html*
(számítógép-biztonság);

*ftp://ftp.win.tue.nl/pub/security*

*http://www.hardbodies.com/creditcardinfo.html*
(hitelkártya biztonság);

*ftp://rtfm.mit.edu*

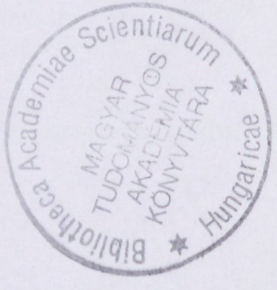
(USENET FAQ-ok, legteljesebb gyűjtemény; közelebbi tükrök is elérhetők, lásd ugyanezen az FTP helyen).

# JEGYZET

JEGYZET

JEGYZET





A NIIF Információs Füzetek sorozatban az alábbi köteteket tervezzük. A címek melletti csillag (*) jelzi, hogy mely füzet készült el.

I. sorozat

1. Rajta vagy már a hálózaton? (*)
2. Kalandozás a Gopherrel
3. Böngészés a WWW-vel
4. Keresgélés a WAIS-szel
5. Gyűjtögetés az FTP-vel
6. Kapcsolattartás e-mail útján az X.25-ön
7. Kapcsolattartás e-mail útján az Interneten
8. Vitatkozás a USENET newsgroupokban
9. Kutatás a hálózati könyvtári katalógusokban (*)
10. Információszerzés kereskedelmi szolgáltatók adatbázisaiból
11. Beilleszkedes a hálózat virtuális világába (*)

12.1 A hálózat használata a molekuláris bológia területén (*)
12.2 A hálózat használata a környezetvédelem területén (*)
12.3 A hálózat használata a számítógépes grafika területén (*)
12.4 A hálózat használata a csillagászat és az űrkutatás területén (*)

13. A hálózat használata a könyvtárakban
14. A hálózat használata az iskolákban (*)
15. A hálózat használata elektronikus publikáláshoz
16. A hálózat használata Windowsból (*)
17. Szórakozás és játék hálózati szoftverekkel

II. sorozat

1. Hogyan csináljunk saját Gophert? (*)
2. Hogyan csináljunk saját WWW-t?
3. Hogyan csináljunk saját FTP archívumot?
4. Hogyan indítsunk saját BITNET/INTERNET levelezőcsoportot?
5. Hogyan indítsunk saját USENET newsgroupot?
6. Hogyan csináljunk saját OPAC-ot?
7. Hogyan integráljuk hálózati információs rendszereinket?
8. Hogyan védjük hálózatra kötött számítógépes rendszereinket? (*)