R. Bruce Miller
University of California, San Diego

Könyvtárak és számítógépek
Katasztrófák megelőzése és kilábalás belőlük*

Jobb félni, mint megijedni – tartja a közmondás. Az állományféltés a könyvtárosok körében ennek megfelelően régi hagyomány. Ehhez társul most – immár hazánkban is – a ránk bízott számítógépes hardver és szoftver, illetve a számítógépekben tárolt adatbázisok féltése. Hogyan féljünk, hogyan féltsünk e tekintetben, s hogyan próbáljuk megelőzni a katasztrófákat – ez most a kérdés. Az University of California munkatársának szellemes írását azért közöljük, mert az USA-ban már nagyobb gyakorlatra tettek szert e kérdések felvetésében és megválaszolásában.

Gondos vizsgálódások szerint a legjobb biztonsági rendszer az, amelyikben a rendszer működtetőin kívül senki sem férhet hozzá semmiféle információhoz. Ezt szem előtt tartva, itt be is fejezhetném.

Komolyra fordítva a szót: van abban némi ráció, ha visszatartjuk a biztonsági helyzetünkre vonatkozó adatokat. Ha a könyvtár bejáratánál elhelyezett hivatalos kinézetű tábla arra figyelmeztet, hogy elektronikus rendszerünk perceken belül riasztja a fegyvereseket, amint rendellenességet észlel, ez éppoly hatékony lehet, mint egy igazi rendszer, viszont minden bizonnyal sokkal kevesebbe kerül. Vagy amikor lerobban az automatizált kölcsönzőrendszer, a legokosabb titoktartást fogadni és ugyanúgy kezelni a fényceruzát és terminált, mintha még mindig regisztrálni tudnánk a kivitt tételeket. Rövid távon minden valószínűség szerint ugyanannyi könyvet hoznának vissza, mint amikor a rendszer valóban működött.

Ez szokatlan bevezetésnek tűnhet, ha az előadás témájára, a katasztrófák megelőzésére és a működőképesség helyreállítására gondolunk, de csak látszólag. Az igazi kérdés a biztonság. Olyan rendszer ugyan nem létezik, amely 100%-ig biztonságos lenne, de előre felkészülhetünk egy sor katasztrófára, így egy viszonylag biztonságos rendszerrel állhatunk használóink rendelkezésére.

Természeti katasztrófák

Tegyük meg hát első lépéseinket a paranoia eme birodalmában, gondolkodjunk el a természeti katasztrófákról és következményeiről. A legtöbb esetben egyszerűen arról van szó, hogy figyelembe kell vennünk azt, ami nyilvánvaló. Ha a tornádó völgyében lakunk, nem fogja-e számítógépünket már az első vihar alkalmából elragadni Óz? Vagy nem a vízvezeték alatt kerestünk-e helyet a komputerünknek? Az egyik régi könyvtárépületben, ahol dolgoztam, a számítógépterem az alagsorba, a gazdasági bejárat mellé, egy hosszú teherautó-feljáró közelébe került. Az esővíz-levezető csőhálózat ugyan jó állapotban volt – de elképzelhető, mire lehetett számítani egy csőrepedésnél. Idegességemet fokozta, hogy azon a vidéken évente átlagosan 152 cm csapadék hullott.

Ami a hirtelen hálózati feszültségingadozásokat illeti – ilyet okozhat például egy közelben becsapódó villám –, attól egy feszültségbiztosító egység óvhatja meg a berendezést, ill. az adatbázist. Aztán itt van a földrengés. Most, hogy Kaliforniába költöztem, ahol nem ritka az ilyesmi, már arra is gondolnom kell, hogy különféle tárgyak megrepednek, eldőlnek, vagy egyszerűen a föld nyeli el őket.

A minimális környezeti követelményeket igénylő kisebb berendezéseket csaknem mindenhol el lehet helyezni, viszont a hagyományos számítógépterem megtervezéséhez kötődő problémák egy mosócédula hosszúságú listává állnak össze, amikor a számítógép helyét jelöljük ki. Könyvtárunk nemrég építette meg második számítógép-létesítményét. Már nem foglalkozunk nagyszámítógépekkel, de van még néhány légkondicionálást igénylő kommunikációs berendezésünk a Kaliforniai Egyetem online katalógusával (MELVYL) való összekapcsolódáshoz. Mivel ezért mindenképpen szükségünk volt egy ilyen helyiségre, elhatároztuk, hogy INNOVACQ és INNOPAC típusú számítógépeinket (amelyek egyébként nem igényelnének légkondicionált helyiséget) ugyanitt helyezzük el, hogy kihasználhassuk a térszervezésből és a hálózati kapcsolatokból fakadó előnyöket. Ez egy ablaktalan helyiség az egyetem központi könyvtárában, kb. 8 m x 8 m, igen magas mennyezettel és vastag betonfalakkal. Először is beszereltünk egy légkondicionáló berendezést. Tudva, hogy leállás esetén ez a típus gyorsan megjavítható, ill. kicserélhető, a tartalék rendszer telepítésétől eltekintettünk. Számításba vettük eközben a betonfalak hőelvezető képességét is, valamint azt, hogy szükség esetén az ajtó kinyitása sem szégyellni való szellőztetési megoldás. Ha nagyszámítógépről lett volna szó, annak sokkal szigorúbb előírásai természetesen nem engedték volna meg, hogy ilyen egyszerűen járjunk el.

*Rövidített fordítás. (Libraries and computers: disaster prevention and recovery. = Information Technology and Libraries, 1988. dec. p. 349–358.)

Tűzriasztó érzékelőt ugyancsak beszereltünk, de megelégedtünk a hagyományos kézi tűzoltó készülékekkel. A korábbi számítógépteremben volt egy halonnal oltó automatikus berendezés, mivel az IBM nagygéphez és egy sor nagy hőkibocsátású, gyúlékony berendezéshez szükség volt rá. Új berendezésünk lényegesen kisebb hőt bocsát ki, és nagyon kevés egysége tűzveszélyes. Így hát a halonos rendszer 10 ezer dolláros költsége plusz a karbantartási költség elriasztott bennünket a védelem e válfajától. Arról nem is beszélve, hogy a halonos rendszer alkalmazása esetén a lerakódott anyag mindenen rajta marad, ami néha több kárt okoz, mint egy idejekorán elszigetelt kisebb tűz. Ráadásul az egészségre is káros, ha egy olyan helyiségbe szorulunk, ahol egy halonnal oltó rendszer lépett működésbe.

Első látásra őrültségnek tűnhet, amit a tüzek eloltása céljából tervezünk. Két év múlva, egy renoválás keretében, vízzel működő tűzoltó berendezéssel látjuk el a helyiséget. Nemcsak a csöveket vezetjük be, amelyek a számítógépek felett lelógva szükség esetén vizet spriccelnek rájuk, de a csőrendszer mindvégig meg is lesz töltve (nem csak tűz esetén, amikor a tűzoltók töltik fel a nyomóvezetékeket). Ez nem olyan ostobaság, mint amilyennek látszik.

A régebbi, vízmentes csöveket alkalmazó rendszereknek két fő problémájuk volt. Üres állapotban csúnya fekete penész fejlődött ki bennük, amely azután rátelepedett mindenre, amikor használni kellett a fecskendőket. (Ez a vizes változatnál is előfordulhat, ha nem áramoltatjuk a vizet, vagy ha néhanapján nem öblítjük át a csöveket.) A másik probléma, hogy könnyebben kilyukadnak, mint a korszerűbb eljárással gyártott berendezések. Az új rendszer képes elzárni magát, ha a tűz sújtotta szoba normális hőmérséklete helyreáll.

A figyelmes szemlélő észrevehette, hogy legalább két évig semmiféle automatikus tűzoltó berendezésünk nem lesz. Mint az egész katasztrófamegelőzési tervezés esetében, itt is kiértékeltük a kockázatot és összevetettük a védekezéshez szükséges kiadásokkal. Az értékelés nyomán arra a következtetésre jutottunk, hogy a tűzvész kicsiny valószínűsége és a gépre kötött biztosítás elegendő biztonságot nyújt mindaddig, ameddig a renováláskor a fecskendőrendszert be nem építhetjük.

A terem padlója alá nedvességérzékelőket helyeztünk el. Ezek még nagyon kis fokú nyirkosság esetén is riasztanak. A helyiség egyik felén fél tucat vízvezetékcső fut végig, a padlótól a mennyezetig. A csövek burkolással vannak ellátva, és a kisebb réseken esetleg kicsöpögő víz az ajtók alatt simán kifolyna a helyiségből. Földrengésnél azonban könnyen törés keletkezhetne, amelynek révén víz ömölhetne a számítógépekre. Ezt végiggondolva, egy védő acéllapot fogunk feltenni a csövek és a számítógépek közé. Ezzel a megoldással aztán a csövek úgy szivároghatnak és fröcskölhetnek, ahogy kedvük tartja, és mégsem ázik el egyik számítógépünk sem.

A számítógépterem alapjában véve egy betonbunker. Becslésem szerint egy akkora földrengés, amelytől megsérülnének az itt levő berendezéseink, valószínűleg az egész könyvtárat romba döntené, mely esetben a számítógép gyors újraindítása nem a legelső gondolatunk lenne.

A számítógép üzemzavarai

A számítógépek tehát már biztonságban foglalhatnak helyet vízhatlan házaikban, de nekünk még mindig izgulnunk kell, nehogy leálljanak. A hardvert kell legelőször stabillá tennünk. Be kell szereznünk egy feszültségbiztosítót (USP), amely tartalékolja a bejövő áramot, hogy a berendezés egyenletes feszültséget kapjon. Az anyagiaktól függően egy átmenetileg tartalék áramgenerátorként is használható berendezésre is szert tehetünk, így a számítógépes rendszer átmeneti leállása nem jár az adatok elvesztésével. Még odáig is elmehetünk, hogy egy valódi tartalék áramforrást szerzünk be, amely helyi áramkimaradás esetén telepről üzemelteti a számítógépet.

A tandem rendszerű számítógépek voltak az első nonstop működésű rendszerek, extra mikroprocesszorral, tartalék operációs rendszerrel és adatbázissal. Ha az egyik processzor meghibásodik, a munka – bár lassabban – tovább folytatódik a másik processzor segítségével. Egy jó többprocesszoros rendszert még a meghibásodott processzor eltávolításának idejére sem kell kikapcsolni. További újítás a tükrözött adatbázis: ebben minden művelet párhuzamosan zajlik le.

Tegyük fel, hogy sikerült folyamatosan árammal ellátni többprocesszoros, tükrözéssel dolgozó rendszerünket, csakhogy – mondjuk – egy villanyszerelő az épület renoválása során átvághatja a számítógépteremből kivezető adatátviteli vonalakat, mert azt hiszi, hogy a régi telefonhoz tartoznak, és az útjában állnak. Huszonnégy órát is igénybe vehetne, míg életet lehelünk a hálózatba. Vajon nem veszítenénk-e el emiatt az állásunkat? Kaliforniában ilyenkor egyszerűen átkapcsolnánk a MELVYL-re, mert olyan szerencsések vagyunk, hogy ez az alternatív online katalógus is a rendelkezésünkre áll. A közeljövőben még a folyóirat-nyilvántartás régi cédulakatalógusához is fordulhatunk (ha pl. mind a MELVYL, mind az INNOPAC működésképtelenné válna), s mire azt selejteznünk kell, addigra remélhetőleg más tartalék forrást is használhatunk, pl. katalógusunk CD-ROM változatát.

Ha az adatbázis eladója mond csődöt

Elsődleges érdekünk, hogy az eladó cég "meghibásodása" esetén hozzáférhessünk az általunk használt szoftver ún. forráskódjához. A szerződésbe ugyan viszonylag könnyen beiktathatunk egy pontot, amely egy semleges harmadik félre bízza a forráskód őrzését és szükség esetén a könyvtárnak való átadását. Ezt persze könnyebb mondani, mint meg-

tenni. A csődbíróság például gyakran visszatartja a forráskódot mint potenciális vagyontárgyat, és akár két évig is elhúzódhat, amíg kézbe kaphatjuk. Addigra a forráskód többnyire el is avul. Egyáltalán tudnánk-e valamit kezdeni a forráskóddal? Mi a számítógéprendszer kiválasztásánál fontos szempontként kezeltük, hogy a forráskódhoz tartozó operációs rendszer és programnyelv nagymértékben szabványosított legyen, és hogy a megfelelő szoftvertámogatás – az egyetem, ill. a könyvtár rendszerszervezői révén – biztosítva legyen.

Osztott rendszerek

Az osztott feldolgozás a katasztrófaelhárítás több gondját megoldja, de új problémákat is teremt. Míg a munkának a különböző helyszínek közötti megosztása csökkenti annak a veszélyét, hogy valamely katasztrófa alkalmával mindent elveszítsünk, továbbá a megosztás eleve párhuzamos kapacitásokat jelent, addig a biztonságot meg is nehezíti, hiszen most több helyiséget és több berendezést kell védelmeznünk. Az osztott rendszerek tulajdonosai gyakran lebecsülik a veszélyt, elhanyagolják a megelőzést.

Biztonság

Vírusok, szalagférgek, trójai falovak

A mágnesszalagférgekről először 1975-ben olvashattunk, *John Brunner* Shockwave rider (Aki lökéshullámon lovagolt) c. regényében, de azóta hasonló kártevések rendszeresen szerepelnek a hírekben. Páciensek adatai tűnnek el kórházi számítógépekből, az elektronikus posta keretében rejtélyes üzenetek olvashatók a képernyőn. Mindezt csúf kis programok idézik elő, amelyek újabban a nagyközönség számára is olcsón hozzáférhetők, és a kereskedelemben kapható szoftverekben is előfordulnak. A számítógépvírusok képesek önmaguk többszörözésére, és megragadnak azon a szoftveren, amellyel kapcsolatba kerülnek. A "trójai faló" (vagy más néven "hátsó bejárat") megbújik egy máskülönben normális program belsejében, és olyan bajkeverő programocskákat szállít, mint a számítógép belső órája által egy adott időpontban aktivizálódó "időzített bomba" vagy az előre meghatározott logikai állapot beálltakor (ill. egy bizonyos billentyű lenyomásakor) robbanó "logikai bomba".

Hogyan védhetjük ezek ellen az adatbázist? Szakértők szerint egy ilyen program becsempészéséhez előbb meg kell nyitni – vagy létre kell hozni – egy fájlt. Akkor vagyunk a legnagyobb veszélyben, ha egy már fertőzött új szoftvert vagy adatbázist veszünk át (pl. a CompuServe nyilvános online rendszerből való "adatletöltéskor"). Ismerni kell a forrást, és az egyes programokat olyan mértékben el kell szigetelni, amennyire csak funkcionálisan lehetséges. A legtöbb könyvtári rendszerben kizárólag a rendszerek karbantartói számára engedélyezik, hogy az állományokat megnyissák vagy létrehozzák. Így ezek viszonylag védettnek tekinthetők, ámbár egy elégedetlen alkalmazott vagy a könyvtár, ill. a szoftvercég valamely nagyeszű munkatársa heccből óriási pusztítást tud véghezvinni. A logika azt kérdezteti velünk: ugyan ki venné a fáradságot, hogy könyvtári adatokat dúljon fel? Sajnálatos módon a logika ebben nem feltétlenül játszik szerepet.

Jelszavak, kódok

Ha bármikor úgy véljük, hogy a jelszavak, a passwordök csak felesleges bosszúságnak vannak, egy percre álljunk meg, és gondoljuk végig, mi lenne, ha valaki elolvashatná a dolgozók munkateljesítményét értékelő jelentéseket, vagy ha egy idegen a könyvtár számlájáról pénzt vehetne fel, vagy ha – és ez a legijesztőbb – a szemünk láttára törlődne egy adatbázis és a hozzá tartozó szoftver – mondjuk – egy logikai bomba hatására. A jelszavakat könnyű használni és karbantartani, az értékük messzemenően ellensúlyoz minden kényelmetlenséget. Néhány egyszerű parancsolat betartása révén a jelszót hasznos eszközzé tehetjük: amint megkaptuk a számunkra kiutalt jelszót, nyomban változtassuk meg; ezután is legalább háromhavonta változtassunk rajta; ha egy csoport tagjai által közösen használt jelszóról van szó, mindig változtassuk meg, valahányszor valaki kiválik a csoportból; ezenkívül is változtassuk meg, amikor csak szükségét érezzük (pl. ha egy demonstráció alkalmával valaki véletlenül megláthatta, amikor begépeltük); a jelszó legalább hat karakter hosszúságú legyen; saját kényelmünk érdekében számok helyett inkább betűket használjunk, lehetőleg két, egymással és velünk semmiféle kapcsolatban nem álló, de azért könnyen megjegyezhető szó kombinálásával; a jelszót memorizálni kell, sehova ne írjuk le (az adatbázisokkal való automatikus összekapcsolódásnál használt bejelentkező program is kockázatos, mivel tartalmazza a jelszót); csak a program jól ismert helyén írjuk be jelszavunkat (ha valamely szokatlan helyen is a jelszót kéri a program, könnyen lehet, hogy a trójai falóval van dolgunk, s az általa hordozott program csak arra vár, hogy a jelszó megszerzése után a bankszámlához férhessen); végül nem árt, ha a számítógép-használatról ugyanolyan részletes naplót vezetünk, mint a banki be- és kifizetésekről.

A biztonság és a hardvertolvaj

A könyvtárgépesítés kezdeti időszakában a számítóközpont személyzete gondoskodott a számítógép fizikai biztonságáról. Most, hogy a számítógépek a könyvtárba kerültek, a felelősség is a miénk. Az Indiana Egyetemen (Indiana University) a könyvtári szövegfeldolgozó rendszerhez tartozó számítógép és adattár a gazdasági bejárat közelében levő helyiségben van. Egy napon valakik odaálltak egy teherautóval, majd azzal, hogy a karbantartó vállalattól jöttek, a számítógépterem iránt érdeklődtek. Várakoztak, míg

a könyvtárosok lázasan keresték a kulcsot. Szerencsénkre azok a valakik nem tudták kivárni, míg a kulcs előkerül, és elhajtottak.

A Kaliforniai Egyetemen (University of California) a biztonsági rendszer illetéktelen behatolás esetén a rendőrséget riasztja. A rendszerhez csak kiválasztott személyek férhetnek hozzá, speciális kártya segítségével. A rendszer finomságai közé tartozik, hogy előre meg lehet határozni, milyen kártyát milyen időszakban fogadhat el a számítógép, továbbá hogy az elvesztett, ellopott, ill. a kilépő dolgozók birtokában levő kártyákat haladéktalanul le lehet tiltani. A számítógépteremnek külön lopásgátló rendszere van, mozgásérzékelő készülékkel, amelyet belépéskor egy kódolt jelszóval lehet lekapcsolni. Meglehetősen kicsi a valószínűsége, hogy egy illetéktelen személy behatolása felderítetlenül maradjon. A berendezések rejtett pontjain egyedi mozgásdetektorokat is elhelyezhetünk. Ezek nem akadályozzák a használatot, sőt a szerelő bele is nyúlhat a gépekbe. De nem tanácsos valamely berendezést közelebb vinni a bejárathoz.

Talpra állás

Tartalék példányok készítése

A legegyszerűbb eljárás az, hogy pár percenként kimentjük azt a dokumentumot, amelyen dolgozunk. Némely szoftver ezt automatikusan elvégzi helyettünk. Azonban továbbra is a mi dolgunk marad a többszörös másolatok készítése, számítva arra, hogy a ma még működőképes mágneslemez holnap már nem enged bennünket az adatok közelébe. Hálózati rendszerben valakinek rendszeresen biztonsági másolatot kell készítenie az állományokból és a használt programokból. Persze, akárhogyan is készítettük el a tartalék példányokat, a továbbiakban róluk is gondoskodnunk kell. Ki-ki gondoljon kedvenc félelmére – tűz, szándékos rongálás, lopás stb. Ne nyugtasson meg bennünket az a tudat, hogy ezeken a mágneslemezeken nincsenek izgalmas adatok. Lehet, hogy csak azért lopnak el egy-egy adatállományt, mert szükségük van a mágneslemezre (amelyhez így felettébb olcsón jutnak hozzá). Az ok végül is közömbös: az elveszett adat elveszett adat marad. Egy tűzbiztos páncélszekrény mindenképpen jó tárolási ötlet.

Az OCLC régen felismerte, hogy első számú tőkéje az online központi katalógus. Egy tíz évvel ezelőtti hírlevélben már azzal büszkélkedett, hogy rendszerhiba vagy egyéb nem várt esemény után egy mikroszekundum alatt minden bibliográfiai rekordot újra tud teremteni, és hogy a rekordokat öt példányban készítik, három különböző helyszínen őrzik, többek között egy külön tűzbiztos épületben és egy másik amerikai állam területén föld alatti raktárban is. A technika fejlődése ezt a szintet is túlhaladta már, viszont az OCLC – igen bölcsen – már nem szolgáltat adatokat biztonsági intézkedéseiről.

Sok könyvtár tekint az OCLC-re mint saját katalogizálási adatbázisának háttérállományára Ez elvileg jogos, de ne ringassuk magunkat a biztonság csalóka illúziójába. Sokba kerülne a tranzakciókat tartalmazó szalagokat az OCLC-re támaszkodva újraalkotni; és akkor is rendbe kellene tennünk a saját adatbázisunkat.

Egyetemünkön régóta készítünk többszörös másolatokat, amelyeket más mágneses adathordozón őrzünk a campus különböző pontjain, sőt újabban már azon kívül is. Hetenként küldjük ki a lemezmásolatokat, s ez a szállító-megőrző szolgáltatás havi 105 dollárunkba kerül. És íme, egy újabb sztori: ez a szolgálat közölte, hogy egyik használónk felmondott egy dolgozójának, aki fel volt hatalmazva rá, hogy különleges alkalmakkor ezt a biztonsági raktárat használhassa. A szolgálatot elfelejtették értesíteni az engedély megvonásáról. Kitalálhatják, mi történt. Búcsúfellépés gyanánt az illető összeszedte és magával vitte az összes biztonsági másolatot.

Van még egy utolsó tanmese. Egyszer a könyvtári rendszerben elromlott a szoftver. A gépkezelő egyenként és módszeresen installálta rajta az adatbázis mindegyik példányát, és nem vette észre, hogy közben mindegyiket tönkretette.

Mikroszámítógépes fájlok helyreállítása

Itt az ideje, hogy az egyensúly kedvéért egy sikertörténetet is elmondjak. A Mankato Állami Egyetemnek (Mankato State University) van egy vizes katasztrófáról szóló díjnyertes története. A vízvezeték a SoftDisk c. szoftversorozat teljes évfolyama felett törött el. Azokat a mágneslemezeket, amelyek egy kicsit vizesek lettek, kézi hajszárítóval gondosan megszárították. A teljesen elázottakat kivették a műanyag borítóból, és tiszta, puha, szöszmentes ruhával törölték szárazra. Üres lemezeket is feláldoztak a lemezborító kedvéért. Ezután minden lemezt új, üres mágneslemezre másoltak át. A csoda az, hogy ennek során mindent sikerült megmenteni, egyetlen adat sem veszett el.

Fájlok helyreállítására különféle segédprogramok kaphatók, a leghíresebb közöttük a Norton Utilities. A helyreállítás lehetőségét az adja, hogy amennyiben egy mágneslemezt ténylegesen újra nem formattáltak, az eredeti állomány még rajta van, csak a címe törlődött le a lemez belső tartalomjegyzékéről. A segédprogram meg tudja találni a fájl kezdőcímét, és rekonstruálni tudja az egész állományt. Rendkívül fontos azonban, hogy mihelyt észrevettük a véletlen törlést, ne használjuk tovább a mágneslemezt, nehogy az esetleges új adatok felülírják a régieket. Itt is érvényes: az adatok rendszeres kimentése sokkal kisebb fáradsággal jár, mint az elveszett fájl rekonstruálása. Hosszabb adatállományokról érdemes több másolatot tartani, több helyszínen, többféle adathordozón. (Mikor ezen az anyagon dolgoztam, minden alkalommal két online másolatot készítettem a szövegről, és a szöveget minden alkalommal papírra is kimásoltam, függetlenül attól, hogy maga a hálózati

szoftver hárompercenként ugyancsak készített egy "backup" példányt, amit mágnesszalagra is kimentett. Ha pedig ez egy igazán értékes dokumentummá sikeredik, a magam számára még floppymásolatot is készítek.) Mindez úgy fest, mintha ágyúval lőnénk verébre, de csak addig, amíg egy hosszabb munkánk el nem illan.

"Melegtartalék" és "üres fészek"

A katasztrófából való kilábalás egyik útja, hogy "melegtartalékot" (hot site) biztosítunk magunknak. A lényeg – *David Rames* nyomán – a következő: egy külön helyen egy komplett számítógéprendszert kell készenlétben tartani. Ha az első számú rendszert lényeges károsodás éri, egyszerűen fogjuk a tartalék adatbázist és a szoftvert, átmegyünk vele a tartalék géphez, és ott folytatjuk a munkát, ahol abbahagytuk. Léteznek erre specializálódott cégek is, amelyek havi potom 2– 6 ezer dollárért szívesen állnak a rendelkezésünkre.

A másik lehetőség, ha megosztozunk egy külső számítógépen, vagy ha kölcsönös segítségnyújtási egyezményt kötünk a hasonló esetektől ugyancsak tartó intézményekkel.

Az "üres fészek" (empty shell) variáció ugyanerre a témára: egy külön helyiséget kell fenntartani, ahol a hardvertől eltekintve minden (áramforrás, távközlés, tároló- és irodalmi helyek) megtalálható. A számítógép-értékesítő céggel kötendő szerződésbe bevehetjük, hogy valamely katasztrófa bekövetkeztekor gyorsan új berendezést küldenek. Az IBM gépek esetében vizsgálati tapasztalatok szerint ez a kiszállítási idő 4 óránál is kevesebb! Az más lapra tartozik, hogy a kézbesítés után az új rendszer "megszelídítése" jó pár napba is beletelik.

Mindkét megoldás igen kényelmes, viszont megnő a rezsi. További gond, hogy a megszokottól eltérő hardver belövése igen nehéz. Emellett nem szabad megfeledkeznünk a hálózati kapcsolatok újbóli kialakításáról, s arról sem, hogy az adatvédelmi problémák is rázósabbá válhatnak az új környezetben. Úgy számolom, hogy a felmerülő költségek és elvégzendő munkák mindkét megoldás esetében meghaladják a legtöbb könyvtár lehetőségeit. Olcsóbb megoldást kell tehát keresni. A "melegtartalék" lehet a hallgatók számára fenntartott mikroszámítógépes laboratórium is, amely felett vészhelyzetben mi rendelkezhetünk, "üres fészeknek" pedig egy bútorraktárként használt helyiség is megteszi. Vegyük ehhez hozzá, hogy katasztrófa ellen biztosíthatjuk számítógépünket (egy 750 ezer dollár értékű számítógépet 2000-ért biztosítanak).

Tervezés

A tervezés az egyetlen biztos pont, amelyre a katasztrófával szemben támaszkodhatunk. Engem néha azzal vádolnak, hogy cassandrai buzgalommal idézem fel mindazokat a veszedelmeket, amelyek a könyvtári számítógéprendszerre leselkedhetnek. Én azonban így tekintek ezekre a dolgokra: ha egy könyvtári adatbázis elvész, vagy ha egy milliós értékű berendezés tönkremegy, nekem és családomnak igen jó kilátása lenne arra, hogy csatlakozzék az otthontalanok seregéhez. Senki sem vonhatja kétségbe, hogy megéri vészmadár hírében állni, sőt egy kis egészséges paranoia sem árt, ha ezáltal biztosítani lehet a stabil jövedelmet és a kaliforniai életstílust.

Talán a legjobb kiindulási pont, ha elfelejtjük, hogy számítógépekről van szó. A cél igazában a könyvtár működőképességének fenntartása. Ez két dolgot jelent: egy tökéletlen terv még mindig jobb, mint semmilyen terv; és: a számítógép és az adatbázis helyreállítása csak része egy ilyen tervnek.

Kenneth N. Myers nyomán a katasztrófaterv kimunkálásának a következő lépései lehetnek:

- a tervezési folyamat megszervezése, a terv kidolgozásával megbízott munkacsoport megalakítása (ki lehet indulni az üzleti és számítástechnikai szakirodalomból, de ne felejtsük el, hogy költségvetésünk nem mindig teszi lehetővé egy tökéletes, hibamentes környezet létrehozását – készpénz híján a kreativitásunkban bízhatunk);
- a lehetséges kockázatok felbecsülése (dokumentálni kell a jelenlegi működési folyamatokat, a tartalék példányok létesítését, a hardverkonfigurációt és a hálózati kapcsolatokat, tekintetbe kell venni a biztosítási szerződést, a használók teljes körét, a fizikai és adatvédelmi lehetőségeket, a lehetséges katasztrófahelyzeteket, fel kell tárni a kritikus műveleteket, miközben igen fontos, hogy akkor kezdjünk hozzá a lehetséges katasztrófák számbavételéhez, amikor Dosztojevszkij-regények olvasása vagy az adóbevallási ív kitöltése révén már megfelelően depressziós hangulatba kerültünk);
- katasztrófaelhárítási stratégiák kidolgozása;
- átmeneti túlélési stratégiák kidolgozása;
- helyreállítási stratégiák kidolgozása (a katasztrófát megelőző állapot visszaállításának lehetőségei és lépései, amihez az egyetlen biztos kiindulópont; nem fogunk hozzájutni egy nagyobb összeghez, hogy újra megvásároljunk mindent);
- az egész folyamat dokumentálása, az egyénekre és feladataikra kiterjedően (fel kell sorolni az új eljárások bevezetéséhez szükséges erőforrásokat, le kell írni a tervet, biztosítani kell, hogy mindenki haszálni tudja).

Fordította: Mándy Gábor