



Illés Zoltán

Számítástechnikai szoftverek – Biztonsági másolatok kezelése, adatvédelem



NSZFI
NEMZETI SZAKKÉPZÉSI
ÉS FELNŐTTKÉPZÉSI INTÉZET

A követelménymodul megnevezése:

Számítógép javítása, karbantartása

A követelménymodul száma: 1174-06 A tartalomazonosító száma és célcsoportja: SzT-041-20

SZÁMÍTÁSTECHNIKAI SZOFTVEREK – BIZTONSÁGI MÁSOLATOK KEZELÉSE, ADATVÉDELEM

ESETFELVETÉS – MUNKAHELYZET

Egyik ismerőse kétségbeesve kéri a segítségét, ugyanis a számítógépe a merevlemez meghibásodása miatt működésképtelenné vált miközben határidős munkáját készítette adatait, eddigi munkáját nem tudja elérni. Az adatok egy részéről rendelkezik másolatokkal pendrive-on, CD-ken, e-mailes levelező fiókjaiban csatolmányokként. Ez az eset ráébresztette arra, hogy adatait átgondoltabban, biztonságosabban kell tárolni.

Abban kéri az Ön segítségét, hogy a meglévő és jövőben keletkező adatainak a tárolásához, kezeléséhez olyan rendszert és módszereket építsenek fel, ami a tárolást biztonságosabbá teszi.

1. Feladat A mentési stratégia kidolgozásához további információkra lesz szüksége. Gyűjtse össze azokat a kérdéseket, amelyre adott válaszok a konkrét terv kidolgozásához kellenek!

SZAKMAI INFORMÁCIÓTARTALOM

BEVEZETÉS

A számítógéppel végzett munka során egyre nagyobb a jelentősége a biztonságnak. Több hónapos vagy éves befektetett munka veszhet el hibás vagy nem létező biztonság politika esetén. Ezt felismerve az egyes intézmények, cégek szabályozottan előírják az adatkezeléssel kapcsolatos szabályokat, melyek betartása a szervezet minden dolgozójára nézve kötelező érvényű.

Számítógép szerelőként, esetenként nagy felelősséggel járó döntéseket kell hozni, olyan műveleteket kell végezni, ami veszélyeztetheti az adatbiztonságot. Az adatvesztések és súlyosabb károk elhárítása érdekében, meg kell ismerni, és tudni kell alkalmazni a biztonságos adatkezeléshez kapcsolódó technikákat, technológiákat.

Ma az információ elérhetősége könnyebb, mint bármikor. Nagy mennyiségű információhoz juthatunk rövid idő alatt az Internet lehetőségeit kihasználva. A szolgáltatók által kínált különféle korlátlan Internet csomagok még inkább feloldják a letölthető adatmennyiségre vonatkozó korlátokat.

A nagy információ éhség az egyéni felhasználóknál is TB méretű adathalmazokat eredményez. A felhasználók sokkal több energiát fordítanak az információ megszerzésére és birtoklására, mint a biztonságos használat körülményeinek a kialakítására. Sokakat csak az olyan az esetfelvetéshez hasonló helyzetek ébresztenek rá a biztonsági mentések és az adatvédelem fontosságára, akik sok munkával elkészített vagy összegyűjtött adatokat vesztenek el.

A hatékony adatvédelem és biztonság kialakítása idő- és költség ráfordítást is igényel, sokan talán ezért sem szánnak rá kellő figyelmet. Mindezek mellett a biztonság kialakításának különböző szintjei valósíthatóak, melyek jellemzőit már nemzetközi szabványok és ajánlások is rögzítik. Az otthoni felhasználók már kisebb időráfordítás árán is jelentősen megnövelhetik rendszerük és adataik biztonságát. A tananyag célja olyan információkat és módszereket bemutatni, amelyek rendszeres és tudatos alkalmazásával a biztonság megnövelhető.

ADATVÉDELEM

A téma kifejtését a tananyag címében szereplő fogalom – az **adatvédelem** – magyarázatával kezdjük. Használjuk jogi és informatikai megközelítésben is.

Jogi megközelítésben:

*"Az adatvédelem a személyes adatok gyűjtésének, feldolgozásának és felhasználásának korlátozásával, az érintett személyek védelmével foglalkozik. Nevével ellentétben tehát nem elsősorban az adatokat védjük, hanem azokat a személyeket, akikkel az adatok összeköthetők. Ennek eszközei lehetnek jogi szabályok, eljárások, de akár technológiai eszközök is."*¹

Informatikai megközelítésben:

*"Az adatvédelem az összegyűjtött adatvagyon sérthetlenségét, integritását, használhatóságát és bizalmasságát lehetővé tevő technológiák és szervezési módszerek összessége."*²

A két meghatározás együttes bemutatása azért is fontos, mert hangsúlyozza, hogy a tananyagban szereplő informatikai, technikai megközelítésen túl a jogi eszközök alkalmazása is jelentős szerepet játszik a megfelelő biztonság kialakításában, melyre a tananyagban is teszünk majd utalásokat.

ADATVESZTÉS OKAI, KÖVETKEZMÉNYEI

Az adatok elvesztését többféle esemény okozhatja, teljesen biztonságos rendszer és technológia nincs. Annak ellenére, hogy az adatok elvesztése reális, több ok miatt előforduló esemény, kevesen foglalkoznak tervezetten, szisztematikusan az adataik biztonságos kezelésével. Sokan sajnálják azt a többlet időráfordítást, ami a biztonságos adattárolási, adatkezelési szokások kialakításához kellene. "Ha már használható, működő a rendszerem miért töltsen a "drága" időmet felesleges további műveletekkel?. Adataim közül csak kevés, ami tényleg nagyon fontos, arról meg úgyis készítek másolatot pendrive-ra!".

Milyen okai lehetnek az adatvesztésnek?

Fizikai, hardveres:

- Hibás működésű eszköz (gyártási hiba, típushiba)
- Túlmelegedés, rossz hűtés
- Por, szennyeződés
- Karcolás, törés, ütődés
- Pára és vízbejutás

Szoftveres

- Alkalmazás összeomlása
- Fájlrendszer sérülése
- Vírustámadás

¹ Forrás : [http://hu.wikipedia.org/wiki/Adatvédelem_\(jog\)](http://hu.wikipedia.org/wiki/Adatvédelem_(jog))

² Forrás: [http://hu.wikipedia.org/wiki/Adatvédelem_\(jog\)](http://hu.wikipedia.org/wiki/Adatvédelem_(jog))

Emberi tényező

- Szándékos vagy hozzá nem értésből adódó károkozás
- Előírt karbantartási és biztonsági szabályok figyelmen kívül hagyása
- Nem rendeltetésszerű használat, (véletlen törlés)

Milyen következményei lehetnek az adatvesztésnek?

- Jelentős anyagi és üzleti károk
- Műszaki vagy egészség károsodást okozó hatások megjelenése
- Presztízs veszteség
- Munkakedv-, motivációvesztés

Az adatvesztés következményeivel, és okaival foglalkozó tudnivalók bemutatásához a legjobb példákat, az adatmentéssel foglalkozó cégek esettanulmányai a szolgáltatják. Egy ilyen hasznos és tanulságos gyűjtemény olvasható a következő internetes oldalon : <http://www.kurt.hu/konyv>

RENDSZER ÁLLAPOTFELMÉRÉS, DIAGNOSZTIKA

Minden javítást állapotfelméréssel, a hiba azonosításával kell kezdeni. Az állapotfelmérés kiterjed az eszközök (hardver) és a rendszer és az alkalmazások (szoftver) helyes működésének ellenőrzésére. Az állapot felmérésnek nagyrészt ugyanezen lépéseit kell elvégezni a javítások után is a javítások sikerességének ellenőrzésére.

Hardver hibák esetén

Az adathordozó hardveres hibájára utalnak a következő jelek:

- az eszközből származó szokatlan zajok, zörejek
- a működést jelző LED diódák nem világítanak
- túlforrósodott eszköz

A mai adattárolók gyártástechnológiájából adódóan, azok hardveres hibái csak speciális eszközökkel és műszerekkel javíthatóak.

Ezért hardveres hibák esetén, ha az adatok fontosak, semmiképpen se próbálkozzunk meg egyéni módszerekkel! Bízunk meg adatmentő céget a javítással! A kísérlet jellegű beavatkozások tovább ronthatják az adatok visszanyerhetőségének esélyeit, ez által drágítják az adatmentő cég által végzett mentés költségeit is! Ilyen esetekben a számítógép bekapcsolása sem javasolt!

Az adatmentő cégek a hibás eszközről elsőként bitenkénti másolatot (képfájlt) készítenek. Az adatok helyreállítását már a másolat alapján végzik az adattöredékek elemzése alapján. Az elkészült mentéseket többnyire optikai adathordozón adják át a megrendelőnek.

Szoftver hibák esetén

Amennyibe a hardver még működőképes, célszerű nekünk is elsőként képfájlt készíteni az adott eszközről! Ezzel a rendszer aktuális állapotát később bármikor vissza tudjuk állítani!

Ezek után próbáljuk meg menteni az adatainkat, ami a fájlrendszer sérülése esetén már nem fog sikerrel járni.

Ekkor próbáljuk meg az operációs rendszer lemez- és fájlkarbantartó segédprogramjait futtatni.

Alkalmazzunk diagnosztikai programokat az adattárolók hibás működésének a felderítésére. A merevlemezek esetén a S.M.A.R.T technológiának köszönhetően az eszköz állapota követhető, a meghibásodás előre jelezhető.

ADATTÁROLÓ ESZKÖZÖK TÍPUSAI

Ebben a részben a témához kapcsolódóan csak áttekintést adunk és az adott tananyag feldolgozásához szükséges speciális ismereteket érintjük. A témával részletesen egy teljesen önálló tananyagelem foglalkozik.

Biztonsági mentéseinkhez többféle adattároló eszközt használhatunk, melyek működési és használati jellemzői különböző módon hatnak a tárolás biztonságára. Az egyes adattárolókat ezek alapján a hatások alapján elemezzük. Elsőként nézzük meg az egyes csoportosítási szempontokat:

Működési elvek szerinti csoportosítás

- Mágneses (merevlemez, floppy, mágnesszalag)
- Optikai (CD, DVD, Blu-ray)
- Elektronikus (pendrive, SSD)

Használati mód szerinti csoportosítás

- A számítógépbe beépített
- Mobil adattárolók (pendrive, CD, DVD, mobil HDD)
- Hálózati adattárolók (helyi hálózati megosztások és meghajtók, NAS, SAN, internetes tárolók, iSCSI)

Csatoló felület és adattárolási mód szerinti csoportosítás

ATA (PATA) csatoló felület: A SATA alkalmazása előtti merevlemez és optikai tárolók csatoló felülete volt. Az ATA felület kialakulásának egy korábbi változataként IDE csatolóként is hivatkoznak rá. Párhuzamos adatátvitelt valósít meg, kényszerűen rövid adatkábel alkalmazásával, emiatt külső eszközök illesztésére nem alkalmas. A mai számítógépekben a SATA felület váltotta fel.

SCSI csatoló felület Az ATA-val egy időben alkalmazott technológia, annál fejlettebb és gyorsabb adatátvitelt tesz lehetővé merevlemez, optikai tárolók és mágnes szalagok számára. Otthoni felhasználásra drága, emiatt vállalati környezetbe terjedt el.

SATA csatoló felület A mai merevlemezekhez és optikai tárolókhoz ezt a felületet használják, a korábbi, ATA (PATA) csatoló felület leváltására szolgál, növelve az adatátviteli sebességet. A SATA a korábbi párhuzamos adatátvitel, helyett vékonyabb vezetékeken soros átvitelt használ. Három jellemző változata van a különböző átviteli sebességek szerint (SATA 1.5 Gbit/s, SATA 3.0 Gbit/s, SATA 6.0 Gbit/s)

USB csatoló felület: Többnyire SATA lemezek számára készítenek olyan külső rack-eket, melyek a SATA felületet jelei az USB felülethez illesztik, így külső mobil HDD-ként használható lesz a számítógép USB portján keresztül.

RAID technológia³: A RAID rövidítés Redundant Array of Independent/Inexpensive Disk, A technológia lényege, hogy **több egymástól független merevlemez együttes használatával** növeli az adatelérési sebességet és/vagy az adatbiztonságot.

Alkalmazása inkább vállalati környezetben jellemző.

Különböző RAID szinteket különböztetünk meg az alkalmazott lemezek számát és a tárolás módját tekintve (RAID0–RAID6, RAID10, RAID01). A tárolás biztonságát többszörözéssel, tükrözéssel, az adatelérés sebességét csíkozással valósítja meg. Alapvetően ezt a két elvet – ,illetve a paritás ellenőrzést– alkalmazzák az egyes RAID változatok. A két elv bemutatására a RAID0 és RAID1 változatokat ismertetjük, melyek tisztán valósítják meg az egyik és másik módszert.

- RAID 0 (csíkozás, összefűzés) Az adatelérés sebességét gyorsítja az által, hogy az adatokat elosztva írja és olvassa az egyes lemezekre, így közel kétszeres lesz (két lemez esetén) az elérhető teljesítmény. Hátrány, hogy nem tartalmaz semmilyen hibatűrés egyik lemez hibája teljes adatvesztést jelent.
- RAID 1 (tükrözés) Az adatbiztonságot növeli az által, hogy több lemezen is ugyanazt a tartalmat tárolja, ez által egy lemez hibája esetén is működőképes marad a rendszer. További előnye, hogy az adatelérési sebességet is gyorsíthatja az által, hogy párhuzamosan tudja olvasni a két lemezt. Megfontolandó lehetőség lehet otthoni felhasználók számára is!

A további RAID szintekről bővebben olvashat a forrásként megjelölt weboldalakon

³ Forrás: <http://hu.wikipedia.org/wiki/RAID>

MILYEN ADATTÁROLÓT HASZNÁLJUNK?

A mentendő adatok mennyiségétől, felhasználásától, a mentés típusától függően választhatunk adattároló eszközt a biztonsági mentések készítéséhez. A következőkben tekintsük át az egyes adattárolók jellemzőit a biztonsági mentésre felhasználhatóság szempontjából.

Merevlemezek: Teljes rendszermentésekhez és adatmentésekhez is jól alkalmazható. A tárolt adatok gyorsan elérhetőek, visszaállíthatóak (a merevlemez működési sebességéből adódóan). A merevlemez a működési elvéből adódóan (aktív elektronikai alkatrészek) sérülékenyebb, mint a leválasztható adathordozók (CD, DVD, streamer). Alkalmazása olyan esetekben célszerű, ahol nagyobb mennyiségű gyorsan, dinamikusán változó adatot kell kezelni. Önálló technológiai megoldásként alkalmazzák a több merevlemezről álló RAID tömböket (részletesebb leírás az előző fejezetben)

Mágnesszalag (steamer) Leginkább vállalati környezetben alkalmazzák teljes rendszermentések és rendszeres ütemezett mentések adattárolójaként. Nagy mennyiségű adat olcsó tárolását teszi lehetővé, viszont az eszköz soros működéséből adódóan az adatok visszaállítása, visszakeresése lassú.

CD, DVD Teljes rendszermentésekhez és adatmentésekhez is jól alkalmazható. A tárolt adatok elérhetősége lassabb, mint a merevlemez esetén, viszont az adattárolás hosszabb távon biztonságosabb lehet, mivel az adathordozó nem tartalmaz mozgó, aktív alkatrészt, ezenkívül a lemezek hordozhatósága miatt, a munkakörnyezettől távol tárolva szintén növeli az adatbiztonságot. Az optikai adattárolók további előnye a káros mágneses hatásokkal szembeni érzéketlenség. Viszont problémát jelenthet a lemezek karcosodása, repedezése, rossz minőségű írható lemezek esetén az anyagszerkezet változásból adódóan a tárolt adatok rövid idejű tartóssága.

Pendrive A számítógép USB csatló felületét használja, így külső, mobil adattárolásra tervezték a floppy lemezek leváltására. Leginkább adatmentésekhez használjuk, bár a jelenleg forgalmazott eszközök kapacitása lehetővé teszi teljes rendszerek mentését is, így ilyen célú alkalmazása is lehetséges. Nagy előnye az adatok mobilitása, könnyű hordozhatósága.

Hátránya az anyagszerkezet változásból adódó korlátozott írási ciklusok száma (kb. 100000 írási ciklus), ezért biztonsági mentések egyetlen tárolójaként nem javasolt.

SSD (Solid State Drive)

A wikipedia meghatározása szerint:

*"Az SSD magyarul szilárdtest-meghajtó, flash memóriás tároló. Félvezetőkkel megvalósított mozgó alkatrészek nélküli adattároló, amely merevlemezként csatlakoztatható a számítógépekhez."*⁴

Az SSD-k alacsony energia felvétel mellett, a merevlemezeknél gyorsabb adatátvitelt képesek megvalósítani, ezért hordozható eszközökbe (notebook, netbook) egyre gyakrabban alkalmazzák háttértárolóként. Hátrányuk a merevlemezekhez képest a magasabb ár, a kisebb tárolókapacitás, a korlátozott élettartam a memóriacellák limitált írás-olvasási száma miatt.

Hálózati meghajtók Többnyire vállalatok, intézmények helyi hálózataiban (LAN) alkalmazzák rendszer- és adatmentés céljából egyaránt. Az adattárolót többnyire egy kitüntetett számítógép a szerver tartalmazza és mint erőforrást osztja meg a hálózaton a munkaállomások számára. A munkaállomások önálló meghajtóként (G:, H:, T:) látják a saját számítógépükön a hálózati meghajtókat.

Jó megoldás lehet kevésbé érzékeny adatok tárolása esetén internetes adattárolókat használni, ennek egyik speciális változata az email postafiókban tárolt csatolmányok alkalmazása.

Például egy segédprogram segítségével a Gmail postafiókhoz rendelt tárterület a számítógépünkön önálló meghajtóként megjeleníthető és használható.

NAS (Network-attached storage)

Hálózathoz csatolt adattároló, melynek használata az otthoni és kis vállalkozások számára is új lehetőségeket hordoz.

A NAS-ok a hálózatra csatlakozó minden számítógép számára biztosítják a szolgáltatásaikat, így például a munka dokumentumok, média fájlok az asztali és a hordozható számítógépekről is elérhetőek, sőt Internet csatlakozás esetén külső hálózatról is használhatjuk!

⁴ Forrás: <http://hu.wikipedia.org/wiki/SSD>



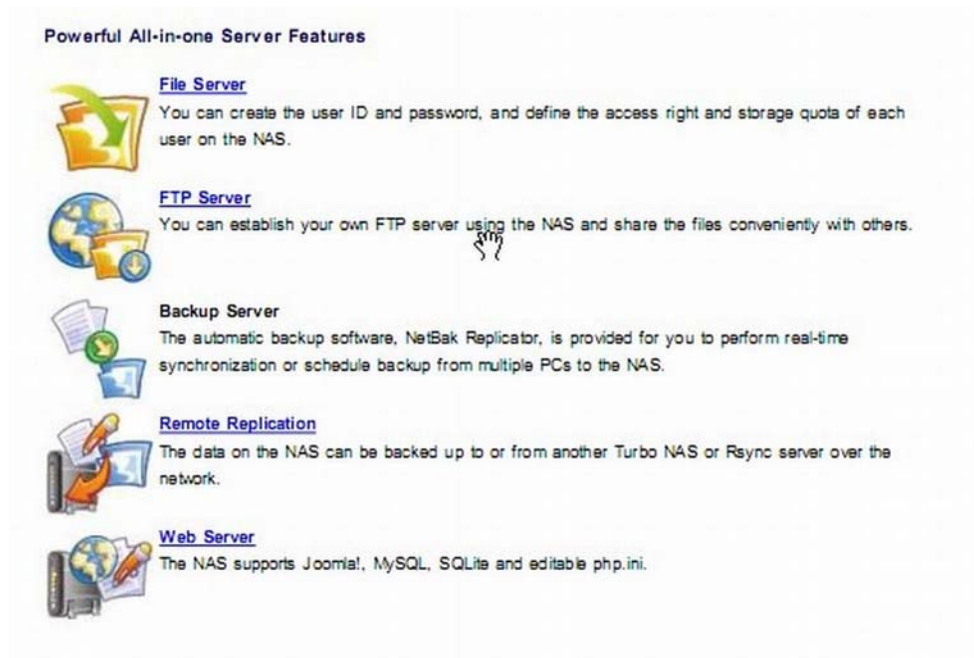
1. ábra TS-119 Turbo NAS

A NAS olyan önálló számítógépként viselkedik, ami speciálisan az adattárolási és kiszolgálási feladatok számára lett kifejlesztve. Saját (többnyire Linux alapú) operációs rendszerrel rendelkeznek, ebből adódóan számos szolgáltatás megvalósítására alkalmasak, melyek frissíthetőek és bővíthetőek. Olyan szolgáltatásokat tartalmaznak, mint:

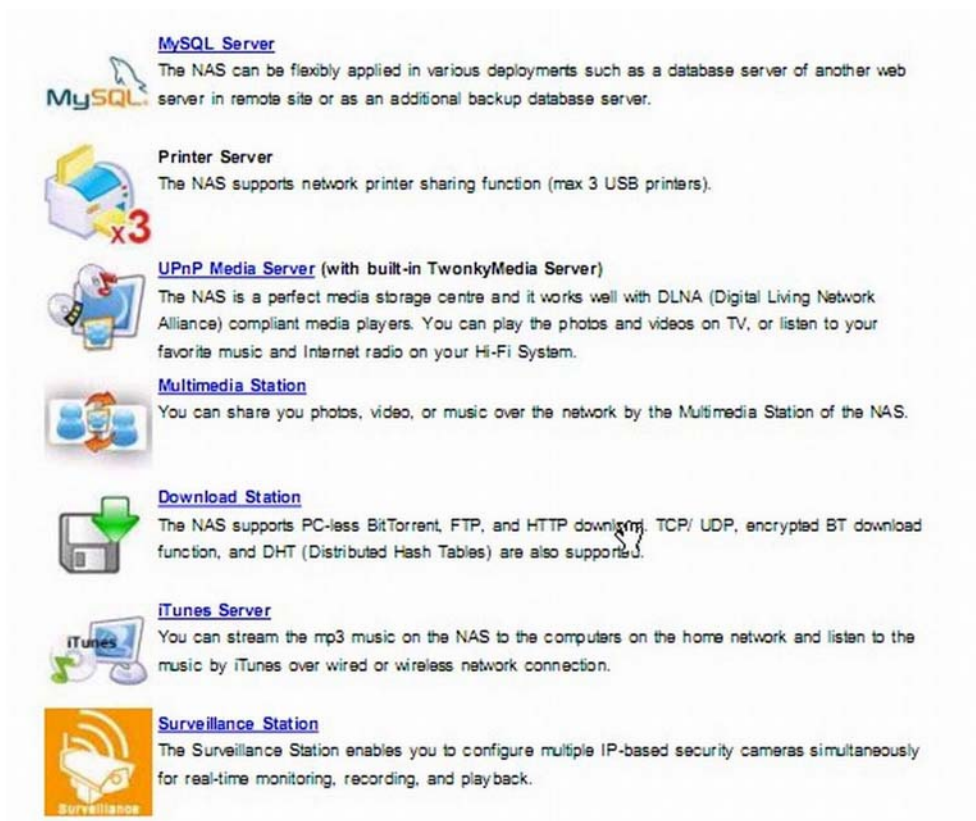
- Fájlszerver felhasználónként beállítható jogosultságokkal, kvótával, jelszavas hozzáféréssel (File Server)
- Beépített ütemezhető letöltés kezelők (Download Station)
- Média szerver fotók, videók, zenék központi tárolására (UPnP Media Server)
- FTP kiszolgálóként használhatóak (FTP Server)
- Web szerver +webes keretrendszerek (Joomla), melyek intranetes portálként üzemelhetnek (Web Server)
- Adatbázis szerver (MySQL Server)
- Nyomtató szerver (Print Server)
- Beépített biztonsági mentés funkciók (Backup Server)
- Biztonsági kamerák adatainak tárolására, megfigyelésére (Surveillance Station)

- S.M.A.R.T funkció merevlemez állapotának figyelésére
- USB eszközként is használhatóak

A következő képeken egy adott termék (TS-119 Turbo NAS) jellemző szolgáltatásai láthatóak *(az angol nyelvű címszavak magyarázata a fenti felsorolásban).*



2. ábra NAS szolgáltatások I



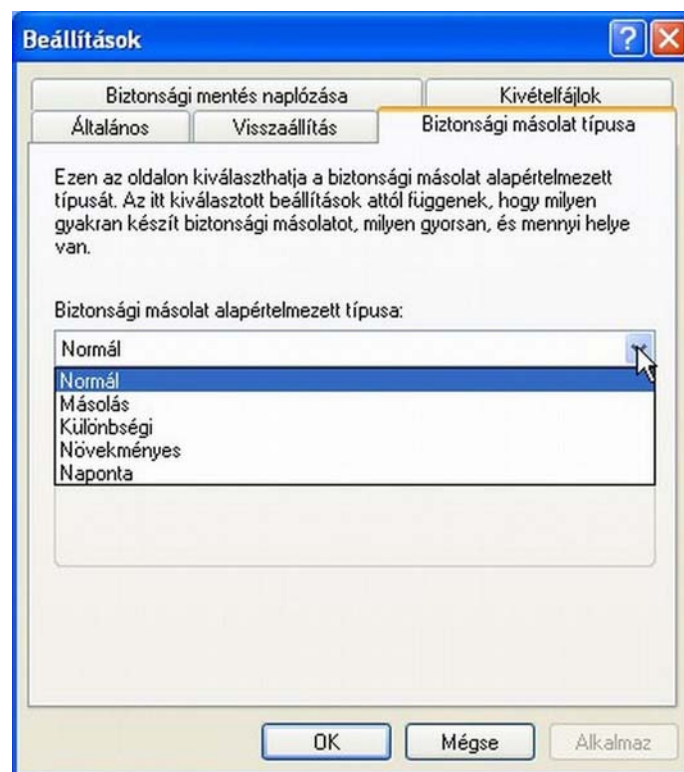
3. ábra NAS szolgáltatások II.⁵

BIZTONSÁGI MENTÉSEK TÍPUSAI

A rendszeres mentések nagy adatmennyiséget eredményeznek, emiatt célszerűbb időszakos teljes mentések között csak a változásokat menteni. A biztonsági mentést végző szoftverek ezt a különböző mentési típusok kiválasztásával teszik lehetővé.

A biztonsági másolatok öt típusát használja a Windows Biztonsági másolatkészítő programja:

⁵ Forrás: http://www.qnap.com/pro_detail_feature.asp?p_id=112



4. ábra mentési típusok

- Másolási
- Napi
- Normál
- Növekményes
- Különbségi

Az alábbiakban áttekintjük ezeket a típusokat, elemezve hogy melyiket mikor célszerű alkalmazni, ezeket az információkat felhasználjuk a megfelelő mentési stratégiák kialakításához.

. Az egyes típusok közötti különbségtétel alapja az, hogy a mentés során a fájlokhoz tartozó archiválandó attribútumot hogyan kezeli a program. A fájlrendszereknél tanult különféle attribútumok közül (rejtett, rendszer, csak olvasható, archiválandó) itt a biztonsági mentések esetén kap szerepet az archiválandó attribútum. Ennek törlése jelöli a mentés tényét, a fájl módosításakor az attribútumot újból jelölté teszi az operációs rendszer.

Másolási biztonsági másolat

Ez a másolat típus az összes kijelölt fájlt átmásolja, de nem jelöli meg a fájlokat, hogy biztonsági mentés készült róluk (más szóval nem törli az archiválandó attribútumot). Akkor célszerű ezt a típust alkalmazni, ha normál és növekményes biztonsági mentés között szeretne biztonsági másolatot készíteni, mivel ez nem befolyásolja ezeket a mentési típusokat.

Napi biztonsági mentés

A napi biztonsági mentés az összes kijelölt, a mentés napján módosított fájlt átmásolja. A biztonsági mentést a rendszer nem jelöli a fájlokon az archiválandó attribútum törlésével.

Normál biztonsági mentés

A normál biztonsági mentés az összes kijelölt fájlt átmásolja, és az összes fájlra jelöli a biztonsági mentés végrehajtását az archiválandó attribútum törlésével. Normál biztonsági másolat visszaállítása esetén elegendő a biztonsági másolat legutolsó példánya. A legelső biztonságimásolat-készlet elkészítésekor általában normál biztonsági másolatot kell készíteni.

Különbségi biztonsági mentés

Minden olyan fájlt átmásol a mentés során, amely a legutóbbi normál vagy növekményes biztonsági mentés óta keletkezett vagy módosult. A biztonsági mentést a rendszer nem jelöli a fájlokon az archiválandó attribútum törlésével. A különbségi biztonsági mentést a normál mentéssel együtt alkalmazzuk. A helyreállításhoz szükség van a legutolsó normál és a különbségi mentésre egyaránt. A mentés alapját a normál mentés képezi, az ehhez képest történt összes változást tartalmazza a különbségi mentés.

Növekményes biztonsági mentés

A növekményes biztonsági mentés, a különbségi mentéshez hasonló azzal a különbséggel, hogy a biztonsági mentés végrehajtását a rendszer jelöli a fájlokon az archiválandó attribútum törlésével. Ez azt eredményezi, hogy a mentés csak a legutolsó normál (első növekményes mentés esetén) vagy növekményes mentéshez képest történt változásokat tartalmazza csak. Az adatok visszaállításához egyaránt szükség van a legutolsó normál és az összes növekményes biztonsági mentésre.

A normál és növekményes biztonsági mentés kombinációjának használata esetén szükséges a legkevesebb tárolókapacitás az adatok biztonsági mentéséhez. Ez biztosítja a leggyorsabb biztonsági mentést. A fájlok visszaállítása azonban időigényes és bonyolult lehet, mivel a biztonságimásolat-készletek több lemezen vagy szalagon lehetnek.

Normál és különbségi biztonsági mentés használata esetén az adatok biztonsági mentése több időt vesz igénybe, különösen gyakran módosuló adatok esetén, de könnyebb az adatok visszaállítása, mivel a biztonságimásolat-készletet a rendszer általában csupán néhány lemezen vagy szalagon tárolja.

ADATMENTÉSI STRATÉGIÁK TERVEZÉSE

A megfelelő stratégia és szabályrendszer kidolgozása összetett, szaktudást igénylő feladat. A kormányzati szerveknél, nagyobb vállalatoknál külön feladatként kell ki dolgozni – akár szervezeti egységekre lebontottan – a megfelelő biztonsági szabályokat az alkalmazandó biztonság politika alapján. A szervezetre vonatkozó biztonsági szabályokat a Informatikai Biztonsági Szabályzat (IBSz) rögzíti, melynek elkészítéséhez szabványok, ajánlások és a vonatkozó jogszabályi háttér gondos áttanulmányozása szükséges. A szakirodalom többszintű biztonságot különböztet meg, a kezelt adatok érzékenységtől és a rendszer működés kritikus jellegétől függően:

- Alapvető biztonság
- Fokozott biztonság
- Kiemelt biztonság

Az esetfelvetésben szereplő helyzet nem indokolja a biztonsági szabályok ilyen részletes kidolgozását. A tananyagban leírt módszerek mégis jelentős mértékben növelhetik az egyéni felhasználók adatainak és rendszer működésének a biztonságát.

Az alábbiakban azokat a szempontokat tekintjük át, melyek szükségesek az adott munkahelyzete vonatkozó, gyakorlatban is végrehajtható mentési stratégia elkészítéséhez.

A biztonsági mentést végző szoftverek beállításait is csak a gondosan megtervezett mentési stratégia alapján lehet sikeresen és eredményesen elvégezni!

A stratégia kialakításához a következő szempontok fogjuk elemezni:

- Munkakörnyezet felmérése
- Mit mentünk? – rendszer és adatmentések
- Mire mentünk? – alkalmazott adathordozók
- Milyen időközönként mentünk? – mentések ütemezése
- Hogyan védjük az adatokat? – térbeli elhelyezés, jogi szabályozás
- Megbízható-e a mentés? – adat és rendszer visszaállítás és ellenőrzése

Munkakörnyezet felmérése

A jó mentési stratégia kidolgozásához minden esetben információra van szükség, az alapján lehet csak választani, döntéseket hozni. A kezelt adatokkal kapcsolatban ismerni kell az alábbi kérdésekre vonatkozó válaszokat:

- Milyen hardver konfiguráción történik az adattárolás?
- Milyen operációs rendszert és fájlrendszert használunk?
- Milyen alkalmazásokat és hogyan fogunk használni (hogyan tárolja az adatait)?
- Milyen adattároló eszközöket, milyen módon (gyakoriság, mobilitás, környezet) használjuk?
- Milyen környezetben történik az adatok tárolása (hőmérséklet, pára, por, mechanikai rázkódás, ütés igénybevétel, mágneses hatások, tápfeszültség viszonyok)

- Külön kiemelném a helyi elektromos hálózat működési jellemzőinek a vizsgálatát
- Hol és hogyan keletkeznek fontos védendő adatok?

A szükséges információk alapján határozzuk meg az alábbi jellemzőket:

- Alkalmazott adattárolók háttértárak (típus, méret, kiépítés, egyéb működési jellemzők)
- Alkalmazott partíció kiosztás és fájlrendszer(ek) meghatározása
- Alkalmazunk-e tömörítést, titkosítást
- RAID alkalmazását igényli-e az adott feladat? Ha igen milyen szintűt?
- Könyvtárszerkezet- és fájlhasználat szabályai a gyors kereshetőséghez
- Mentési típus és időzítések meghatározása (bővebben a mentési típusoknál)
- Mire mentünk? Egy vagy többféle médium használatára van szükség/lehetőség?
- Hol találhatóak a fontos mentendő adatok?
- A rendszer biztonságát, hogyan védjük? (tűzfal, vírusellenőrzés, backup, rendszer képfájlok)
- Ki(k) végzi(k) a mentést?

Írjuk le a helyreállítás menetét olyan módon, hogy az alapján kevésbé képzett szakember is el tudja végezni a helyreállítást.

Végezzünk próbamentést és visszaállítást (bővebben korábbi fejezetekben), ennek eredményeit dokumentáljuk.

A mentési stratégia tervezése során alapvetően az **adatok helyreállításának** megbízhatóságát és időigényességét kell szem előtt tartani!

Mit mentünk? – Rendszer és adatmentések

Különböző stratégiát alkalmazunk az adatok és a rendszerfájlok mentése során. Az adatok épségének, felhasználhatóságának biztosítása, ellenőrzése egy jóval egyszerűbben behatárolható feladat, mint a rendszert működtető elemek hiba esetén történő helyreállítása.

Adatmentés szempontjai

Az adatok tárolására célszerű kialakítani egy a munkánkhoz és az adatkezelési szokásainkhoz illeszkedő könyvtár szerkezetet, illetve meghatározni a fájl- és könyvtár elnevezési szabályokat. Ezek a szabályok segítik elő a mentendő és helyreállítandó adatok elkülönítését, gyors megtalálását.

A kategorizálásnak többféle szempontja lehet, amit egyrészt a szerkezet, másrészt az elnevezések tudatos használatával lehet megvalósítani.

Kategorizálási szempontok lehetnek a következők:

- Dátum szerint
- Témakör szerint

- Felhasználás szerint (egy feladat során kezelt adatok egy helyen)
- Fájl- adattípusok szerint
- Adatok érzékenysége, biztonsága szerint

A kategorizálási szempontokat nekünk kell kiválasztani a kezelt adatok mennyiségétől és használati módjától függően. Néhány konkrét javaslat a kategorizálás módjának kiválasztására:

- Projekt munkák esetén az egy feladathoz tartozó adatokat célszerű egyben kezelni, a könyvtárban belül fájl típusonkénti elkülönítést célszerű alkönyvtárak használatával megoldani.
- Hang, kép, video állományokat célszerű témánként könyvtárazni (például zenei, filmek, oktató anyag, természet)
- Bizalmas információkat, melyek személyes adatokat tartalmaznak célszerű külön könyvtárba helyezni titkosítani, jelszóval védeni a hozzáférést.
- A családi eseményeket tartalmazó fotókat, videókat, célszerű dátum szerint kategorizálni.

Rendszermentés szempontjai

A rendszermentések alapvető célja a helyreállíthatóság biztonsága és gyorsasága, ezt kell alapvetően szem előtt tartani!

Lehetőség van teljes és részleges rendszermentéseket készíteni. Az operációs rendszer új telepítése és jelentősebb változtatása –új alkalmazások, új hardver telepítése– esetén mindig célszerű teljes mentést készíteni, melyet időszakos részleges mentésekkel egészítünk ki a kisebb változások megtartásához.

A teljes mentésekhez érdemes lemezkép készítő szoftvereket is használni, mint például a Norton Ghost vagy a Linuxon futó Partimage, Az így készült képfájlok alapján lehet a leggyorsabban elvégezni a rendszer helyreállítását.

Az egyes biztonsági mentés típusokról a "Mentés típusok" fejezetben olvashat bővebben

Mire mentsünk? – adathordozók kiválasztása

A mentéshez használt adathordozók kiválasztása részben technikai részben anyagi kérdés. A technikai jellemzők mérlegeléséhez és az adott munkakörnyezetben történő alkalmazhatósághoz adtunk szempontokat az adathordozókról szóló részben.

Az anyagi ráfordítás mérlegelésekor ne csak az árat, hanem az általa megszerezhető **biztonságot** és a fejlesztéssel nyerhető **további szolgáltatásokat** is vegyük figyelembe!

A biztonság növelése a meglévő adathordozók és technikai eszközök jobb szervezésével, használatával is elérhető (például rendszer és adat partíció szétválasztása). A mentési stratégia kialakításakor törekedjünk a meglévő lehetőségek jobb kihasználására

Milyen időközönként mentsünk? – Mentések ütemezése

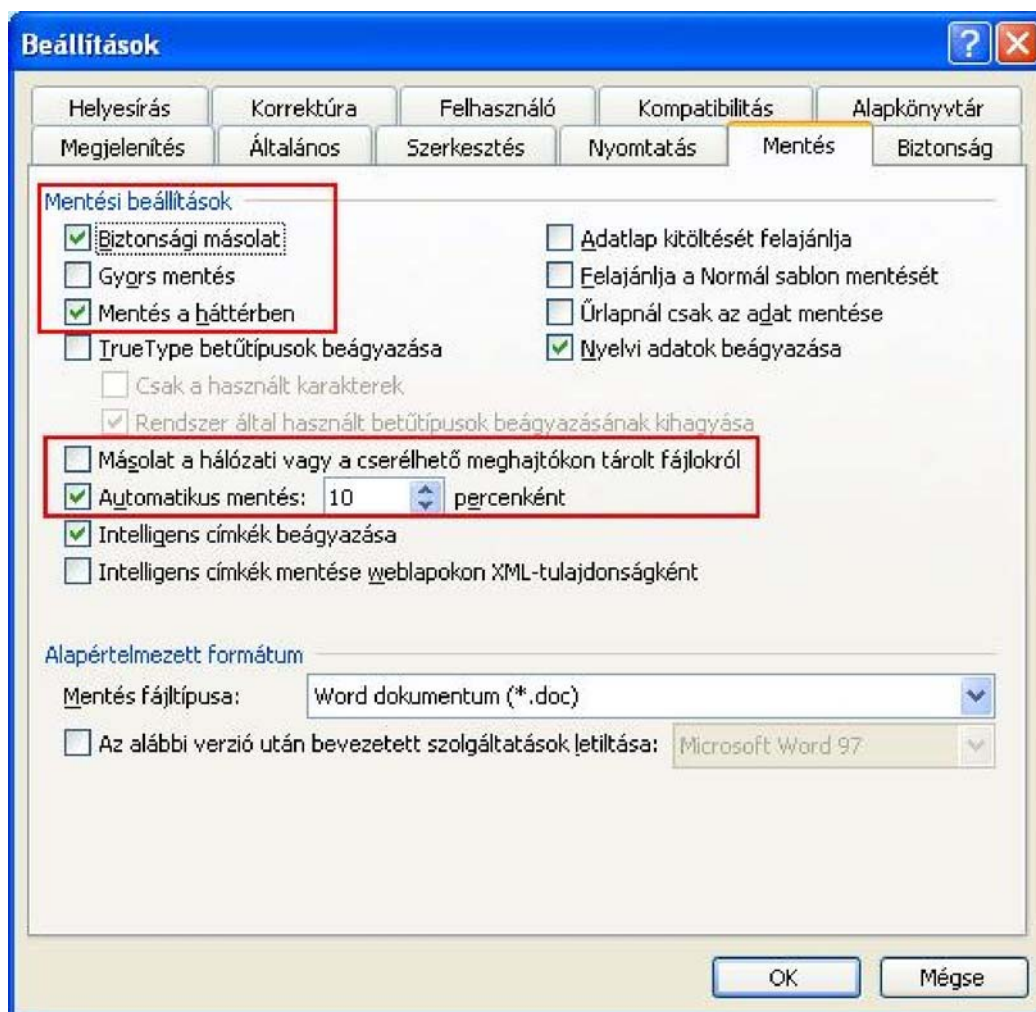
Az adatok használati-, módosítási gyakoriságától függően határozzuk meg a mentések ütemezését. A teljes rendszermentéseket érdemes minden jelentősebb hardver-, illetve szoftvertelepítés vagy átkonfigurálás előtt, és után elvégezni. A munkaadatok esetén is a befektetett munkaórák függvényében, illetve a jelentősebb módosításokhoz igazítottan célszerű menteni.

Néhány javaslat a felhasználáshoz igazodóan a mentések ütemezésére:

Felhasználás	Ütemezés
Otthoni használatú munkaállomások rendszer mentései	2 havonta, illetve jelentősebb szoftver vagy hardver változások esetén
Munkadokumentumok aktív munkafolyamatban	automatikusan 20 percenként, vagy kéziként jelentősebb adatbevitel és módosítás esetén
Szerverek helyi hálózatban (web, mail, ftp)-	napi mentések éjszakai órákban

Ha a munka során a különböző fájlváltozatokat készítünk, a fájlok elnevezése és elhelyezése során tervszerű, tudatos szabályokat alkalmazzunk. Célszerű lehet a fájl változatok követésére külön adminisztrációt is vezetni. Ez alapján a mentési folyamat több egymáshoz kapcsolódó művelet együttes elvégzését jelentheti (átnevezés, mentés, áthelyezés, adminisztrálás). Ez biztosítja, hogy a mentések alapján a fájlok változásai követhetők legyenek.

A mentések időzítése automatizálható, az egyes alkalmazások és a biztonsági mentést készítő programok is lehetőséget adnak az automatikus mentések időzítésének a beállítására! Ezek a beállítások sok bosszúságtól menthetnek meg minket a napi munkáink során!



5. ábra A Word mentési lehetőségeinek beállítása

Hogyan védjük az adatokat? – Térbeli elhelyezés, jogi szabályozás

A káros környezeti hatások (tűz, víz, pára, mágneses tér), lopás, rongálás kivédése szempontjából fontos, hogy a biztonsági másolatok térben (helyiségekben, földrajzilag) is megfelelően legyenek elhelyezve.

Az adathordozók ismertetésénél részben már kitértünk ezekre a szempontokra is. Ha az adathordozókat ebből a szempontból vizsgáljuk, akkor a másolandó adatoktól való távolságuk növekedésével az adatbiztonság is növekszik. Ezt foglaljuk össze az alábbi táblázatban:

Alkalmazott adattároló	Távolság a munkaadatoktól	Biztonsági szint
Beépített merevlemez	Adatokkal egy helyen (0 m)	kicsi
Mobil adattárolók, CD, DVD, pendrive	Adatokkal egy helyiségben, épületben (2–10m)	közepes
Hálózati meghajtók, NAS	Adatokkal egy épületbe, azonos hálózatban (5m–2km)	nagy

Internetes tárolók	Adatoktól külön hálózatra (akár több ezek km)	nagy
--------------------	---	------

A távolság növelésén túlmenően, korlátozni kell az adatok hozzáférhetőségét is, hogy illetéktelen személyektől, káros hatásoktól fizikailag is védve legyenek. A korlátozásokat a technikai eszközök és biztonsági berendezések alkalmazásán kívül, jogi eszközökkel is szabályozni kell!

Az adatok védelme és hozzáférhetőségének szabályozhatósága, az informatika technológiájából adódóan egyre inkább jogi kategóriává is válik, – ahogyan a tananyag elején utaltunk is erre – melyet helyi, nemzeti és nemzetközi szabályok rögzítenek.

Megbízható-e a mentés? – adat és rendszer visszaállítás, ellenőrzés

Ahogy korábban is kiemeltük a biztonsági mentések készítésének a fő célja az adatok helyreállíthatósága!

Valós biztonságot csak az jelent, ha adatvesztés vagy a rendszer összeomlás esetén a munkakörnyezetet a biztonsági mentések alapján helyreállítható!

A helyreállításokat is célszerű rendszeres ütemezéssel, megfelelő stratégia szerint végezni! A sikeres helyreállítások után érezzük igazán a biztonsági mentések készítésébe fektetett energiáink megtérülését.

A kudarcok pedig rámutatnak azokra a pontokra, ahol változtatásokat kell végrehajtani a kialakított mentési stratégián. Tehát **a mentési stratégia kidolgozása nem egyszer végrehajtott folyamat eredménye, hanem a helyreállítás során szerzett tapasztalatok által folyamatosan változik és javul!**

ADATVÉDELMI SZOFTVEREK JELLEMZŐI

Az adatvédelemmel kapcsolatos műveletek végrehajtásához speciális alkalmazások, segédprogramok készültek. Röviden tekintsük át az egyes szoftvertípusok jellemzőit.:

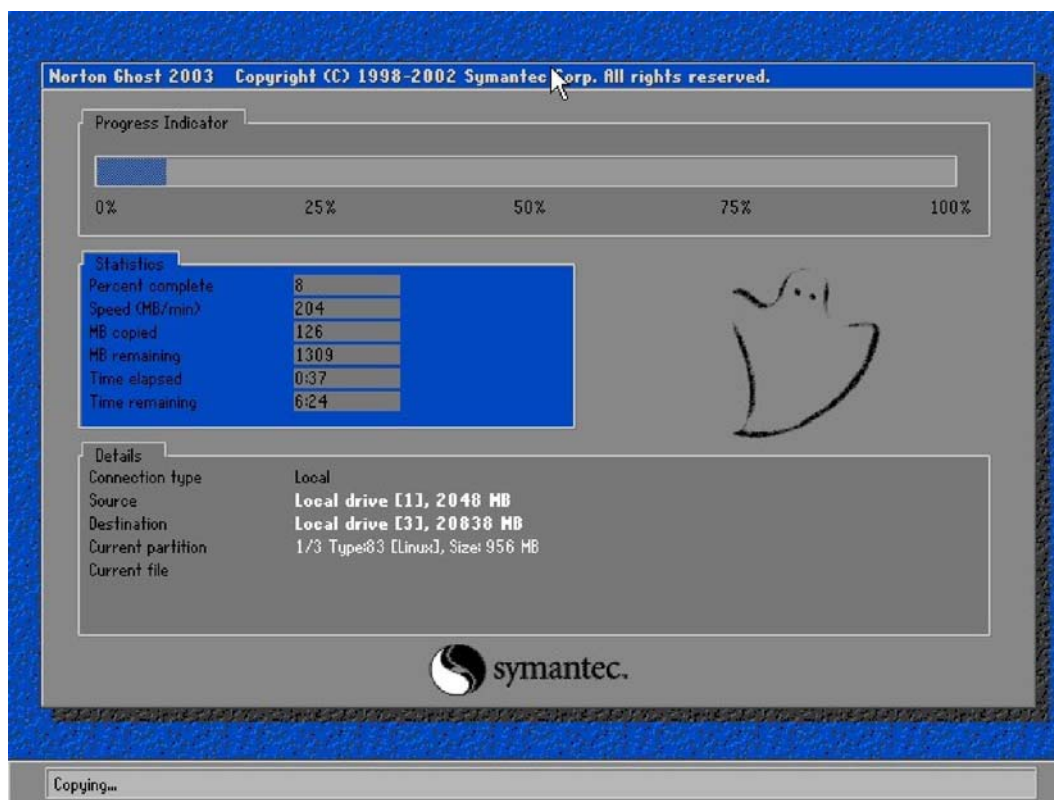
Adathelyreállítók (data recovery)

Egy adott fájlrendszer hibáinak javítását tudja elvégezni, a fájlrendszer felépítését, sajátosságait figyelembevevő algoritmusok alapján.

Lemezkép készítő (disk image, disk clone)

A teljes merevlemezről vagy CD, DVD lemezeről készít **bitenkénti másolatot**, melyet **önálló fájlban** (image vagy képfájl) tudunk tárolni és onnan helyreállítani.

Teljes rendszer mentések esetén javasolt a képfájlok használata, ez alapján a teljes rendszer percek alatt visszaállítható a mentett állapotnak megfelelően. Itt kell megemlíteni a Norton Ghost programját, ami ebben a kategóriában talán a legelterjedtebb kereskedelmi termék. Lehetőséget biztosít teljes lemezek, vagy partíciók mentésére és helyreállításra több féle céllal, illetve forrásból (másik lemez, képfájl, hálózati meghajtó). A program segítségével egy teljes telepített rendszer percek alatt helyre állítható (Windows XP + alkalmazások 4,2 GB os telepített méretben image alapján 5 perc alatt visszaállítható).



6. ábra Norton Ghost lemezmentés közben

Adatmegsemmisítők

Az operációs rendszer által elvégzett törlés parancs nem alkalmas érzékeny, bizalmas adatok megsemmisítésére, egyes helyreállító szoftverekkel sok esetben az adatok viszonylag nagy része visszanyerhető. Érzékeny adatok megsemmisítését csak többszöri törléssel, speciálisan erre a célra kifejlesztett programokkal lehet elvégezni.

Lemezhiba előrejelzés, állapotfigyelés (S.M.A.R.T), diagnosztikai programok (HDD Health)

A merev lemezek számára kidolgozott S.M.A.R.T technológiának köszönhetően a keletkezett hibák száma, előfordulási gyakorisága alapján megbecsülhető a merevlemez várható élettartama. Ezen felül a lemezek működési paraméterei (fordulatszám, hőmérséklet) is megfigyelhetők működés közben, Számos a S.M.A.R.T technológia adatait felhasználó merevlemez diagnosztikai programmal találkozhatunk.

Biztonsági mentés szoftverek (Backup)

Adatok és rendszerfájlok mentését és helyreállítását végezhetjük el kézi vagy ütemezett végrehajtással. A mentésre és a helyreállításra szánt könyvtárak és fájlok szabadon kijelölhetők, amivel a mentéseket az igényeinknek megfelelően testre szabhatjuk. Többféle adathordozó lehet a mentés és a helyreállítás forrása.

A tananyag alapvető célja, hogy ezen szoftverek, megismeréséhez és használatához szükséges ismereteket és módszertani útmutatásokat adjon. A következő rész egy ilyen biztonsági szoftver használatát mutatja be részletesen.

A WINDOWS XP BIZTONSÁGI MÁSOLAT SEGÉDPROGRAMJA

A Windows Biztonsági másolat segédprogramja alkalmazható adataink és a rendszer állapotának mentésére és visszaállítására is. Az esetleírásban szereplő rendszer biztonsági szintjének növeléséhez alapvetően ezt a programot fogjuk használni. A használatához szükséges ismereteket találjuk meg ebben a fejezetben, a biztonsági mentés és helyreállítás lépéseit bemutatva.

A szoftver alkalmazása során nem az adott program kezelőfelületének ismerete a lényeges, hanem a program funkcióinak tudatos és tervszerű használata, ez biztosítja a könnyű áttérést más hasonló funkciókkal rendelkező programok alkalmazására!

A tananyag a Windows XP operációs rendszerre készült változatot ismerteti, de korábbi és későbbi Windows változatok is tartalmazzák a biztonsági másolat segédprogramot, az itt leírtak azokra a változatokra is nagy részben alkalmazhatóak.

A program lehetőségei, funkciói:

- Kijelölt fájlok és mappák archiválása, másolása merevlemezre, vagy más külső adathordozóra (mágnesszalag, pendrive, hálózati meghajtók).
- Az archivált fájlok és mappák visszaállítása az eredeti helyükön túl, másik könyvtárba vagy adathordozóra is lehetséges.
- A teljes rendszerösszeomlás utáni visszaállításhoz szükséges rendszerfájlok és konfigurációs beállítások mentése és visszaállítása az automatikus rendszer-helyreállítás segítségével.
- Másolat készítése a távtárolókon és a csatlakoztatott meghajtókon lévő adatokról.
- Másolat készítése a számítógép rendszerállapotáról
- Másolat készítése a számítógép rendszerpartíciójáról, rendszerindító partíciójáról és a számítógép vagy a hálózat meghibásodása esetére a rendszer indításához szükséges fájlokról.
- Biztonsági másolatok rendszeres készítése az archivált adatok naprakészen tartása érdekében.
- Parancssoros futtatási lehetőség, feladatok automatizálása, ütemezése szkriptekkel

- A varázsló üzemmód felhasználóbarát beállítási lehetőséget kínál a műveletek elvégzéséhez

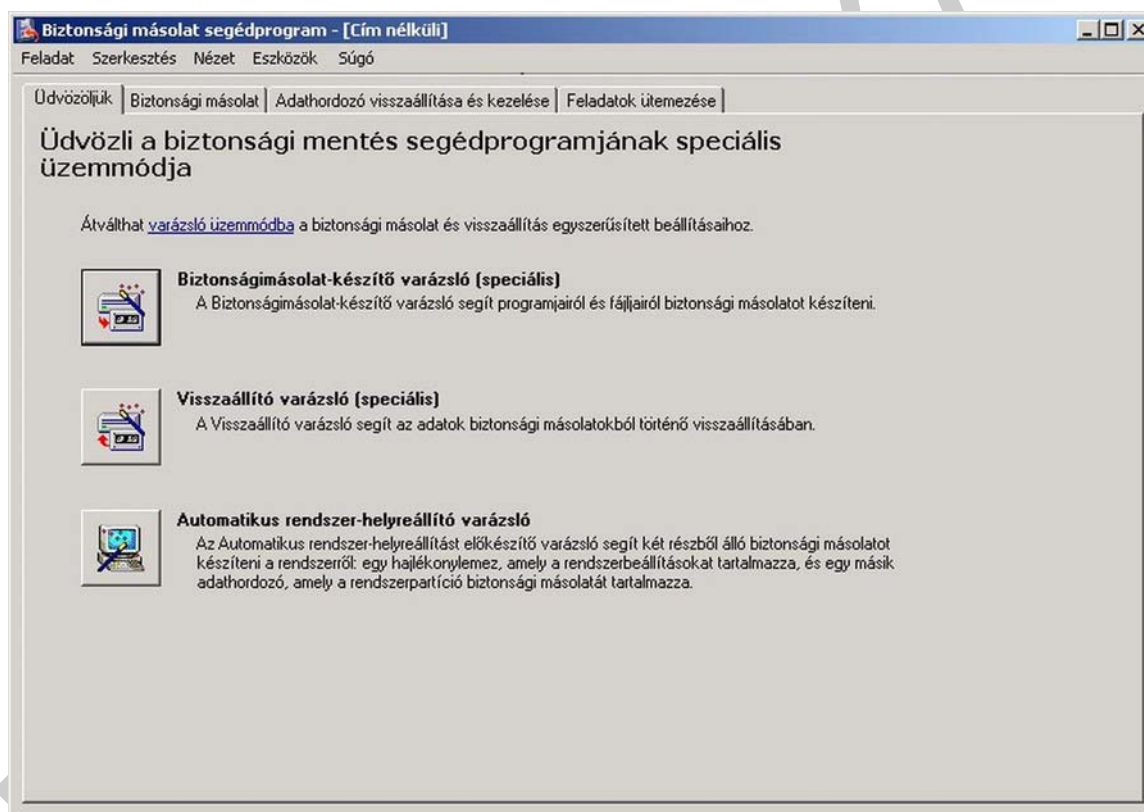
A következőkben áttekintjük a program főbb funkcióit a használat sorrendjébe:

A program indítása

A program indítható a **Start menü/Minden program/Kellékek/Rendszerezszközők/Biztonsági másolat** elérési útvonalon

Vagy a Start menü/Futtatás ablakába vagy a parancssori terminál ablakba az **ntbackup** parancs begépelésével.

Az alkalmazás indítóképernyője az alábbi ábrán látható:



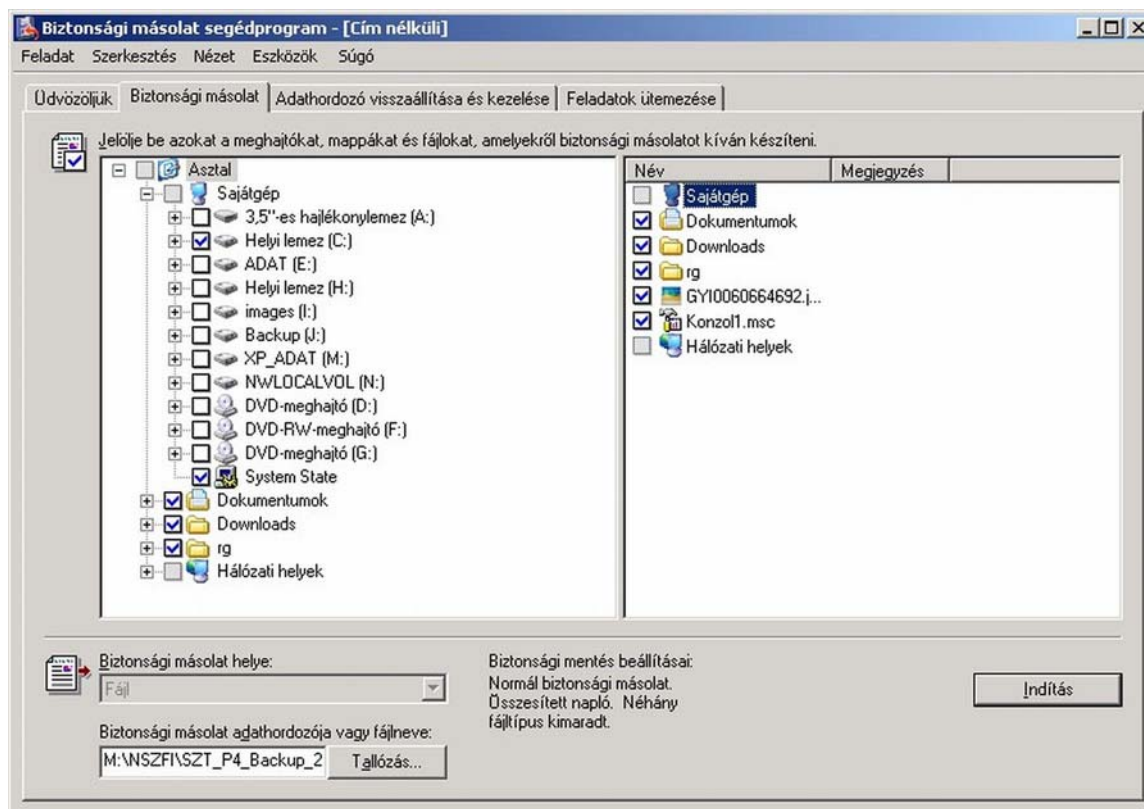
7. ábra A Biztonsági másolat segédprogram indítóképernyője

Adatok (fájlok és mappák) kijelölése mentésre

A "Biztonsági másolat" fülön tudjuk kijelölni a mentésre szánt adatokat a fájl- vagy könyvtárnév előtt álló jelölőnégyzet kiválasztásával.

A **rendszer helyreállításához** szükséges adatok mentését a – alábbi ábrán is kijelölt – **System State** tétel kijelölésével érhetjük el. Ez **több GB szabad tárkapacitást is igényelhet** a cél meghajtón!

A mentendő adatok szerkezetének, elnevezéseinek kialakításához, használjuk az előzetesen elkészített mentési stratégiában szereplő könyvtár és fájlkezelési szabályokat!



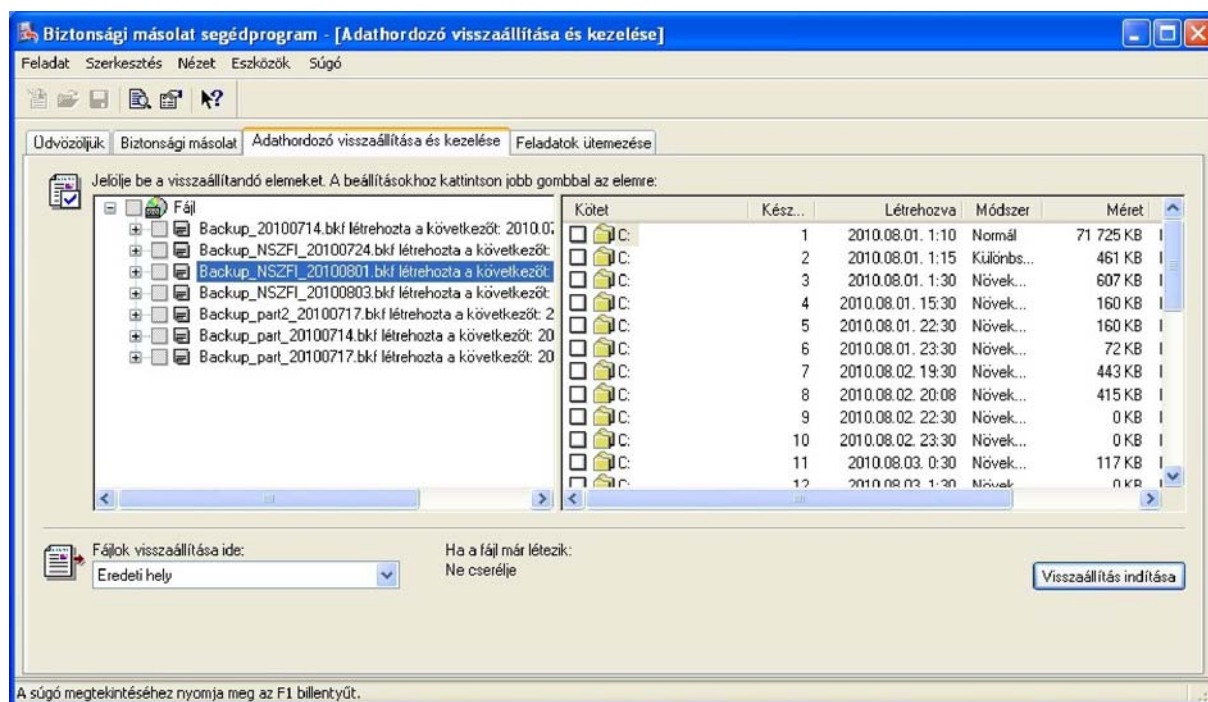
8. ábra Mentendő fájlok és mappák kijelölése

Mentés helyének, céljának kijelölése

Az előző ábra bal alsó részén adhatjuk meg a mentés helyét, a megfelelő meghajtó és könyvtár kiválasztása után kell megadnunk a biztonsági másolatot tartalmazó fájl nevét.

A biztonsági másolat fájl .bkf kiterjesztésű speciális állomány, ami a mentett adatokon túl, azok eredeti tárolási szerkezetét és a mentés egyéb körülményeit tartalmazza, ez teszi lehetővé a visszaállítás pontos végrehajtását!

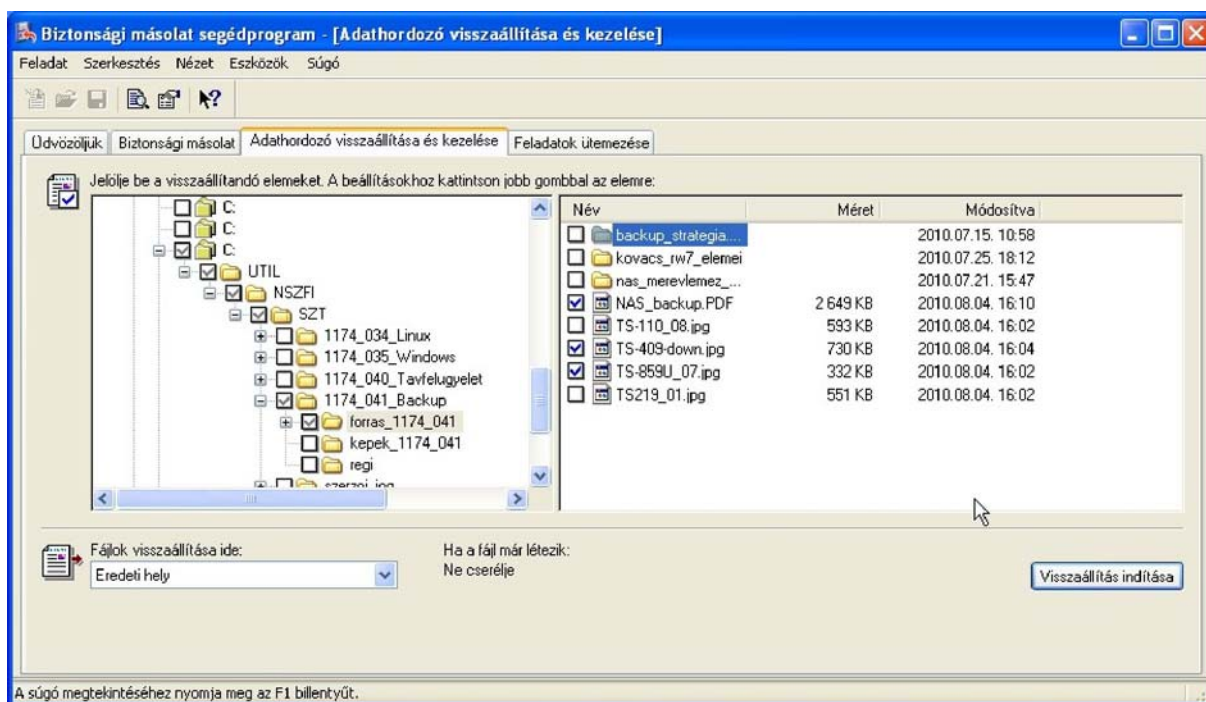
Az alábbi képen azokat a speciális mentési információk láthatóak, amelyeket csak a biztonsági másolat fájl (*.bkf) adatai alapján jeleníthetünk meg. Ez teszi igazán hasznossá és kényelmessé a program használatát! Többek között láthatók az egyes mentések típusai, dátumai, a mentett adatok mérete, így lehet a helyreállítandó adatok visszakeresése gyors és egyszerű művelet.



9. ábra

Adatok (fájlok és mappák) helyreállítása

Az adatok helyreállítása az "Adathordozó visszaállítása és kezelése" fülön végezhető el a biztonsági mentés fájlok alapján. Megadhatjuk a visszaállítandó fájlokat és könyvtárakat, valamint azt is, hogy az eredeti helyükre vagy másik mappába kerüljenek a visszaállítás után.



10. ábra

Feladatok ütemezése

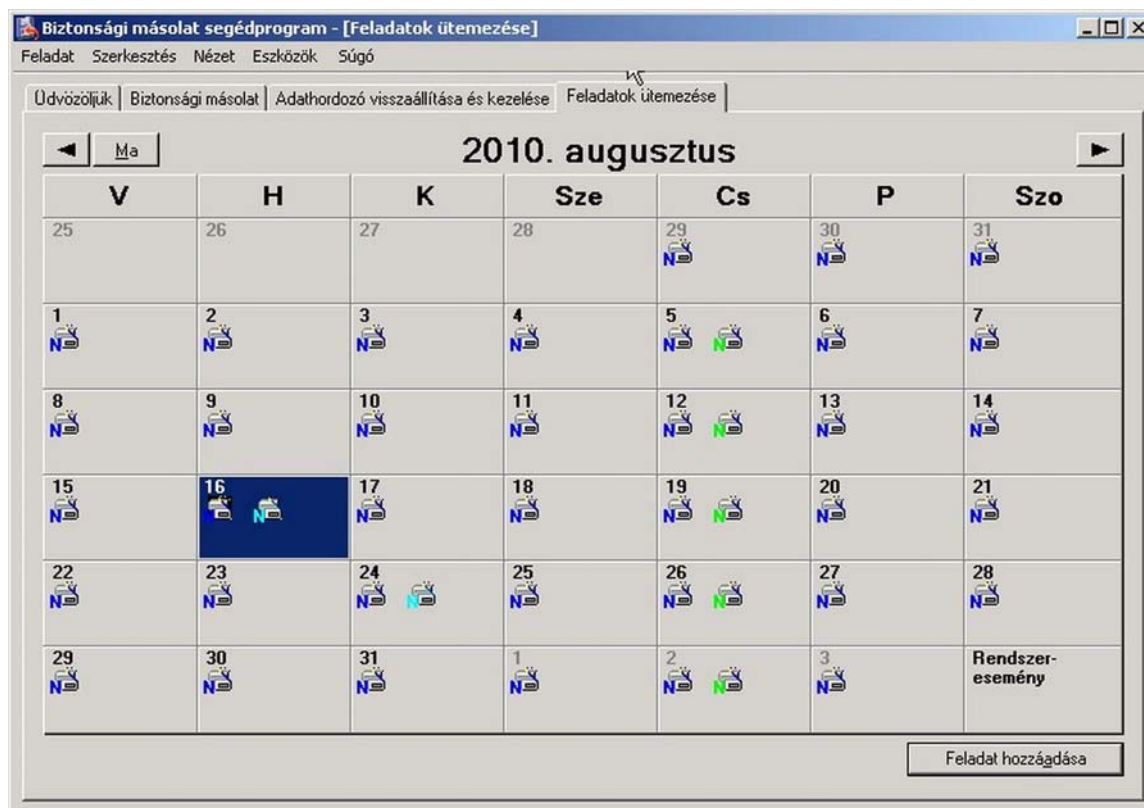
A "Feladatok ütemezése" fülön tudjuk megtekinteni és elvégezni a szükséges beállításokat.

A mentési feladatok ütemezését a Windows Feladatütemező szolgáltatásának felhasználásával tudjuk megvalósítani. A mentési jellemzők beállítása után a mentések végrehajtását a Windows külön szolgáltatása fogja elindítani a megadott időpontokban.

Az ütemezett mentések csak akkor hajtódnak végre, ha a számítógép az adott időpontban be van kapcsolva!

Akár több különféle típusú mentés is ütemezhető különböző gyakorisággal!

Az alábbi ábrán háromféle mentési típus látható. (A *növekményes napi*, a *különbségi minden csütörtökön és két normál adott időponthoz kötve*)



11. ábra

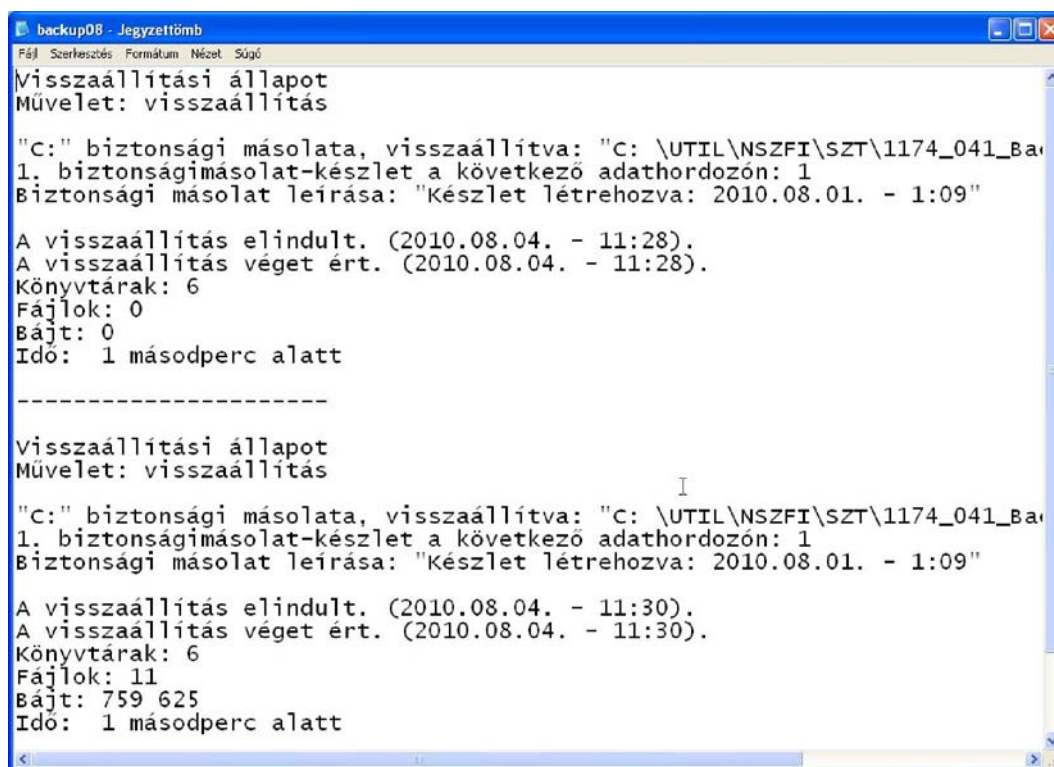
Naplózási lehetőségek – Jelentések

A mentések eredményeit és jellemzőit a program szövegfájlokba (Jelentések) rögzíti. Ezek adatai alapján, a mentés során felmerülő hibák helye és ideje is behatárolhatóvá válik.

Az alábbi képek a Biztonsági mentés segédprogram naplózási funkcióit mutatják be.



12. ábra Választható naplófájlok



```

backup08 - Jegyzettömb
Fájl Szerkesztés Formátum Nézet Súgó

Visszaállítási állapot
Művelet: visszaállítás

"C:" biztonsági másolata, visszaállítva: "C: \UTIL\NSZFI\SZT\1174_041_Ba
1. biztonságimásolat-készlet a következő adathordozón: 1
Biztonsági másolat leírása: "Készlet létrehozva: 2010.08.01. - 1:09"

A visszaállítás elindult. (2010.08.04. - 11:28).
A visszaállítás véget ért. (2010.08.04. - 11:28).
Könyvtárak: 6
Fájlok: 0
Bájt: 0
Idő: 1 másodperc alatt

-----

Visszaállítási állapot
Művelet: visszaállítás

"C:" biztonsági másolata, visszaállítva: "C: \UTIL\NSZFI\SZT\1174_041_Ba
1. biztonságimásolat-készlet a következő adathordozón: 1
Biztonsági másolat leírása: "Készlet létrehozva: 2010.08.01. - 1:09"

A visszaállítás elindult. (2010.08.04. - 11:30).
A visszaállítás véget ért. (2010.08.04. - 11:30).
Könyvtárak: 6
Fájlok: 11
Bájt: 759 625
Idő: 1 másodperc alatt

```

13. ábra Egy naplófájl tartalma

Hibaelhárítás

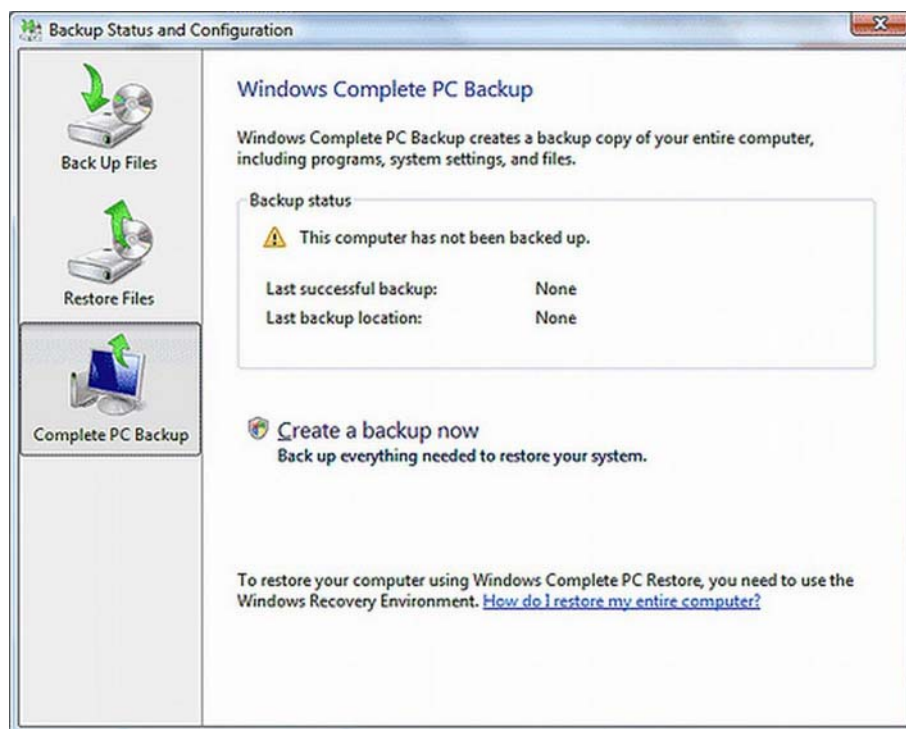
A sikertelen mentés esetén az alábbi hiba okokat vizsgáljuk meg:

- A mentési célként kijelölt adathordozó megtelt-e?
- Sérült-e a fájlrendszer a forrás vagy cél meghajtón?
- Megfelelő típusú-e a fájlrendszer a forrás vagy cél meghajtón (FAT, NTFS) ?
- A mentést végző felhasználó jogosultságai elegendőek-e?
- Helyes volt-e a könyvtár és fájl kiválasztás a mentés vagy helyreállítás során?
- A kijelölt adathordozó betűjele változott-e a mentési beállításokhoz képest?
- Ütemezett mentés esetén, adott időpontban a számítógép be volt-e kapcsolva?
- Az adott (különösen mobil) adathordozó csatlakoztatva volt-e a számítógéphez?

BIZTONSÁGI MENTÉSEK WINDOWS VISTÁVAL

A Windows Vista több biztonsággal kapcsolatos funkciója is változott, bővült a Windows XP-hez képest, így többek között a biztonsági mentések terén is hozott újításokat.

Nemcsak a kezelőfelülete változott, másik programot írtak erre a feladatra. Ezért a korábban XP alatt készült biztonsági mentésfájlokat (.bkf) sem tudja kezelni, ahhoz az XP *ntbackup* segédprogramjára lesz szükség .



14. ábra Windows Vista biztonsági mentés segédprogramja

A Vista két legfontosabb újdonsága közül az első, hogy bármilyen, akár **optikai adathordozókra** (CD, DVD) is tud **menteni**, másrészt a rendszerről **képfájlt (image)** tud **készíteni**, melyet a telepítőlemezrel helyre lehet állítani,

ÖSSZEFOGLALÁS

A tananyag feldolgozása során bemutatott információk segítenek abban, hogy az esetfelvetésben szereplő munkahelyzetet megoldjuk, és egy biztonságosabb munkakörnyezetet teremtsünk.

Az itt leírt ismeretek akkor válnak igazán hasznossá, ha a gyakorlatba is alkalmazni tudjuk őket. Ebben segít módszertani tanácsokkal a következő rész, a Tanulásiirányító.

TANULÁSIIRÁNYÍTÓ

A tananyag, az esetfelvetésben szereplő munkahelyzet megoldásához szükséges ismereteket és módszereket tartalmazza. Az ismeretek nagy részét a szakmai ismeretanyagból bemutatottuk. Ebben a részben olyan módszertani kiegészítéseket adunk, amelyek segítenek az itt megadott feladatok elvégzésében.

Az alkalmazott módszerek, technológiák idő- és költség ráfordítást is igényelnek. Emiatt az adott munkahelyzetre alkalmazható megoldásoknál, az egyedi sajátosságokat is mindig figyelembe kell venni!

Nem egyszerű egy adott munkakörnyezetre kialakítani és alkalmazni a megfelelő biztonsági és adatvédelmi technikákat! Több összetevője van a feladat elvégzésének, melyeket az információs részben igyekeztünk bemutatni. Az adott munkakörnyezet biztonsági szintjét az alkalmazott technológiák és módszerek összessége fogja meghatározni.

Fontos, hogy a biztonságosabb munkakörnyezet kialakítása, nem egyszeri tevékenység eredménye. A biztonság politikában és a mentési stratégiában meghatározott elveket, szabályokat rendszeresen kell alkalmazni és ellenőrizni, ez szemléletváltást is igényel az eddig kialakított munkamódszerekhez képest!

Tanácsok az adatmentési tervet készítéshez

A terv elkészítéséhez a szakmai információ tartalomnál szereplő útmutatást kövesse. A hiányzó információk megszerzése további kutató munkát igényelhet, melyekhez az irodalomjegyzéket és tananyagban szereplő hivatkozásokat is felhasználhatja. Az adatmentési tervet annyira dolgozza ki, hogy az esetfelvetésben szereplő helyzetre alkalmazható, gyakorlati útmutatást jelentsen. Az esetfelvetésből nem meghatározható információkra tegyen egyéni javaslatot, az adott munkahelyzetnek megfelelően.

Hogyan gyakorolja a biztonsági mentések készítését?

Készítsen biztonsági mentés az Ön által használt rendszerről! Határozza meg a rendszer és az adatok szempontjából fontos munkakönyvtárakat, ezeket jelölje ki archiválásra az adatmentő szoftverben. Végezze el az adatok mentését pendrive-ra! Dokumentálja a mentési folyamatokat egyéni jegyzőkönyv formájában az adatmentő szoftver naplózási adatainak felhasználásával.

Határozza meg egy adott biztonsági mentés elvégzéséhez szükséges idő- és tárterület igényt! Milyen feltételek szükségesek még az ütemezett biztonsági mentés feladat sikeres elvégzéséhez?

A tananyag elemben a Windows XP Biztonsági másolat segédprogramjára térünk ki részletesen. Ennek használatát, jellemzőit tekintjük át olyan feldolgozásban, hogy ez alapján az esetfelvetéshez kapcsolódó feladatokat meg tudjuk oldani a szoftver használatával.

A szoftver alkalmazása során nem az adott program kezelőfelületének ismerete a lényeges, hanem a program funkcióinak tudatos és tervszerű használata, ez biztosítja a könnyű áttérést más hasonló funkciókkal rendelkező programok alkalmazására!

Hogyan elemezze a munkahelyzetre alkalmazható mentési módszereket?

Készítsen táblázatos formában elemzést az egyes biztonsági megoldások alkalmazásának bemutatására. Térjen ki az alkalmazhatóság feltételeire, költségeire, mikor ajánlja a módszert! Használjon internetes forrásokat is konkrét adatok begyűjtéséhez.

Hogyan gyakorolja az adatok helyreállítását?

A kapott biztonsági másolat alapján végezze el az adatok vagy a rendszer helyreállítását. A helyreállítás előtt mérje fel a rendszerállapotát.

Legyen körültekintő a helyreállításnál, nehogy adatvesztést okozzon abban az esetben, ha a meglévő rendszert egyes elemeit változatlanul kell hagyni!

TANULÁSI TERV

Az alábbiakban a tananyag elsajátításához szükséges elvégzendő feladatokat lépésekre lebontva adjuk meg. A feladatokat az adott sorrendben célszerű végrehajtani az alkalmazható tudás megszerzéséhez.

Fontos kihangsúlyozni, hogy a feladatok elvégzése nem csak a leírt információk elsajátítását, megtanulását jelentik, hanem a kijelölt gyakorlati feladatok tényleges elvégzését is! Ennek hiányában a munkavégzéshez szükséges készségek nem alakulnak ki.

A gyakorlati munka során számos olyan jellegű információ és ismeretanyag meg jelenik, ami tisztán elméleti úton nem elérhető. Például egy adott mentési folyamat időszükségletének vagy tényleges tárigényének meghatározása, ami a valós költségek tervezése során alapvető jellemzők.

– Biztonsági másolatok kezelése, adatvédelem

- Elemesse az esetfelvetésben szereplő munkahelyzetet! Keressen a témához kapcsolódó internetes forrásokat!
- Ismerje meg az adatvesztés okait és következményeit!
- Ismerje meg a különböző adathordozók jellemzőit, biztonsági másolat készítésre való alkalmazhatóságuk szempontjait!
- Ismerje meg a biztonsági szabályzatok kialakításához ajánlott módszereket, szabványokat!
- **Készítsen különböző munkahelyzetekre és konfigurációkra mentési stratégiát!**
 - **Elemesse a munkahelyzetet a megvalósítandó biztonság politika szempontjából!**
 - **Határozza meg a mentéshez használandó adattárolókat!**
 - Határozza meg az alkalmazott mentési típusokat és azok ütemezését!
 - Határozza meg a biztonsági mentéshez alkalmazott szoftvereket!
 - Elemesse az elkészült stratégiát idő- és költség ráfordítás szempontjából, szükség esetén hajtson végre módosításokat!
- Ismerjen meg és próbáljon ki különböző adat- és rendszermentő, biztonsági másolatkészítő szoftvereket!

- **Készítse elő a következő lépésekben a munkakörnyezetet a biztonsági másolatok készítéséhez:**
 - Határozza meg és csatlakoztassa a számítógéphez mentésre használt adattárolókat
 - Telepítse, ellenőrizze a biztonsági másolat készítő szoftver alapbeállításait (jogosultságok, helyes működés)
 - Ellenőrizze a mentéshez használt eszközön a rendelkezésre álló szabad terület nagyságát!
- **Készítsen biztonsági másolatokat az Ön által tervezett mentési stratégiának megfelelően!**
 - Állítsa be a mentendő (forrás) adatok helyét
 - Állítsa be a mentés (cél) helyét!
 - Állítsa be a mentés típusát és egyéb opcióit!
 - Állítson be a mentési stratégiának megfelelő feladat ütemezést!
 - Készítsen kézi és ütemezett másolatokat a fenti beállításoknak megfelelően!
 - Elemesse a biztonsági másolat készítés során keletkezett jelentéseket, riport fájlokat!
 - Ellenőrizze visszaállítással a mentés sikerességét!
- Rendszeresen alkalmazza a saját munkakörnyezetéhez illeszkedő mentési stratégiát!
- Oldja meg az Önellenőrző feladatokat!
- Végül pedig az informatika felgyorsult fejlődését is szem előtt tartó fontos tanács:

Képezze tovább magát az Irodalomjegyzékben szereplő források és a témához kapcsolódó internetes és nyomtatott folyóiratok írásai alapján!

ÖNELLENŐRZŐ FELADATOK

1. feladat

Miben különbözik az adatvédelem informatikai és jogi megközelítése?

2. feladat

Az alábbi technikai leírás egy háttértárra vonatkozik, mit derít ki a leírás alapján?

Seagate Momentus 7200.4 500GB (ST9500420AS) SATA-II, 7200 rpm, 2,5"

3. feladat

Adja meg az alábbi biztonsági mentéssel kapcsolatos műveleteknek helyes sorrendjét, az előttük szereplő betűk megfelelő sorrendben történő megadásával?

- A : mentési stratégia készítés _____
- B : biztonsági mentés ütemezett végrehajtása _____
- C : adatok helyreállítása _____
- D : munkakörnyezet elemzése _____
- E : biztonsági mentést végző szoftver beállítása _____

4. feladat

Készítsen adatmentési tervet az esetleíráshoz!

5. feladat

Milyen esetekben célszerű lemezkép készítő programokat használni?

6. feladat

Milyen szempontokat vesz figyelembe ütemezett mentések kialakításánál?

MEGOLDÁSOK

1. feladat

Az adatvédelem **informatikai** megközelítésben a védelmet megvalósító **technológiákkal, módszerekkel**, a **jogi** pedig az **adatokat kezelő személyekkel** foglalkozik.

2. feladat

500 GB tároló kapacitású, SATA csatoló felületű, 2,5" lemez átmérőjű, 7200 1/min fordulátú merevlemez jelöl

3. feladat

D–A–E–B–C.

4. feladat

Minta terv

Az eseteíráshoz kapcsolódó adatmentési tervhez szükséges adatok:

Számítógép konfigurációja:

- Intel Pentium 4 1700 CPU
- HDD SATA 160GB 7200 rpm (beépített)
 - 100GB (NTFS) Windows Vista bussines
 - 10GB (NTFS) Windows XP Professional SP2 operációs rendszer
 - 20 GB (EXT2) Ubuntu 8.04 LTS
 - 1 GB (SWAP) cserepartíció
 - Maradék 29 GB(FAT32) ADAT
- HDD SATA 80GB 7200 rpm (mobil rackbe)
 - 40GB (NTFS) Windows XP Professional SP2 operációs rendszer
 - 20 GB (FAT32) ADAT
 - 20 GB (FAT32) BACKUP rendszer képfájlok, biztonsági mentések
- RAM SDRAM 512 MB (2*256)/133 MHz
- Beépített Toshiba DVDRW meghajtó
- 4 USB 1.1 port

2 db USB 2.0 pendrive 4GB Datatravel és 8 GB Kingston

Adathasználati szokások felmérése:

A számítógép napi rendszerességgel használatban van Internet használat (web, email) céljából, ez 40–50 MB napi letöltött adatforgalmat jelent. Heti két–három alkalommal készít 3–4 órán át elektronikus formában többnyire szöveges dokumentumokat, prezentációkat, melyeket pendrive-on vagy e-mailben továbbít a munkahelyére. A dokumentumok mérete 1–5 MB. Rendszeres biztonsági mentéseket nem végzett, a fontosabb adatait pendrive-ra mentette, illetve email postafiókjába van róluk másolata.

A mentések tárolásához a felhasználástól függően létrehoz újabb könyvtárakat, de ezek elhelyezése, elnevezése összességében nem rendszerezett

Lehetséges adatmentő tárolók:

A beépített merevlemez meglévő vagy újra kialakított partíciói dinamikus, változó adatok biztonsági mentéséhez biztosíthatnak első szintű védelmet, melyet más adathordozók alkalmazásával tehetünk teljesebbé

A meglévő mobil rackben lévő 80Gb-os merevlemez.

A két meglévő esetleg további pendrive-ok felhasználhatóak

Az email postafiókon kívül internetes tárolók is felhasználhatóak

Jó lehetőség lehet a ma elterjedőben lévő NAS meghajtók használata, ez kisebb beruházást igényel, viszont rugalmas adattárolást tesz lehetővé a későbbiek során, hasznos szolgáltatásokkal kiegészítve az otthoni informatikai rendszert

Írható CD és DVD lemezek is használhatóak időszakos nagyobb mentésekhez

Szalagos tárolók használata nem célszerű ilyen jellegű adathasználathoz

Adatmentési stratégia

Ütemezés

A munkadokumentumokat célszerű 20–30 perceként menteni, esetleg automatikus mentést beállítani. Nagyobb terjedelmű dokumentumok esetén biztonsági másolatokat is készíteni ugyanazon mappába (a Word mentés beállításainál ez automatizálható)

Az Internet használat során letöltött adatokról célszerű kategorizálás után heti két alkalommal növekményes mentést, havonta teljes mentést készíteni.

A munka dokumentumok könyvtáráról (MUNKA) heti egy teljes mentést és napi több alkalommal növekményes mentést célszerű készíteni.

Fájl és könyvtár használati konvenciók

A munkaadatok és letöltések tárolásához egy önálló adat partíción célszerű MUNKA és LETOLTES könyvtárakat létrehozni, ezeken belül további alkönyvtárakba csoportosítani témánként az adatokat.

A fájlok és könyvtárak elnevezése utaljon a tartalomra (Például Fotok, szerzodesek, konyveles, Tervrajzok_2010). Az olyan azonos jellegű adatok esetén, ahol gyakran megjelennek újabb változatok a névbe építsük be a dátumot és a verziószámot (például Nyaralas_2010_julius könyvtár, vagy Olasz_100725_012.jpg képfájl). A számok és dátumok alkalmazása, azért is célszerű, mert könnyebbé teszi a visszakeresést. A fájl és könyvtár nevekbe NE használjunk ékezeteket, különösen, ha másfajta fájlrendszerekben is tároljuk, használjuk az adatokat. Szóközök helyett is a "_" (alulvonás) használata ajánlott.

Hová mentünk?

Az adatok elsőszintű biztonsági mentéseit célszerű a beépített merevlemez egy elkülönített partíciójára menteni. Az adatmentések mellett ide kerülhetnek a rendszermentések is. A biztonsági mentés partícióját célszerű NTFS (Windows) vagy ext3 (Linux) típusúra választani a fájlrendszerek robusztussága, jobb hibatűrő képessége miatt.

Második szinten külső adathordozókat használhatunk gyakrabban változó adatokhoz USB pendrive-ot, nagyobb időközi mentésekhez CD vagy DVD lemez használata ajánlott. Az időzített mentésekhez használjuk a mobil rackbe épített 80GB-os merevlemezt.

A sok munkaráfordítással készült kevésbé bizalmas adatokat internetes meghajtókon vagy email csatolmányként is tároljuk el.

Amennyiben hajlandóak vagyunk beruházni a biztonság érdekében használjunk NAS hálózati adattárolót, ezzel kiegészítő szolgáltatásokat és jövőbeli rendszerbővítési lehetőséget is biztosíthatjuk.

Adatmentő szoftver kiválasztása

Az adatmentésekhez a Windows beépített Biztonsági másolat segédprogramját használjuk.

A rendszermentéshez lemezképet készítünk a Norton Ghost vagy a Linux-os Partimage segédprogrammal.

A mentések fizikai elhelyezésének módja

Az adatokat fenyegető fizikai károk (tűz, víz, lopás) miatt, mindenképpen el kell különíteni térben is az egyes másolati példányokat. Ezt három szinten valósítjuk meg:

1 szint A számítógéppel egybeépítve, másik lemezen, vagy partíción

2 szint Külső adathordozókon, de ugyanabba a helyiségbe, épületbe (például pendrive, CD, DVD, NAS)

3 szint Távoli helyen, másik épületben vagy szerveren (például CD, DVD, NAS, internetes adattárolás)

Az egyes mentések elnevezésében szereplejen a mentések dátuma, verziószáma.

5. feladat

Teljes rendszermentésekhez használhatjuk:

- telepítés után,
- jelentősebb konfiguráció változtatás esetén
- rendellenes, hibára utaló hardver működés esetén
- több azonos konfigurációjú számítógép telepítéséhez

6. feladat

- milyen mentés típusról van szó
- mekkora mennyiségű adatot eredményez?
- mennyire érzékenyek, bizalmasak a mentendő adatok?
- milyen időrendben és milyen kihasználtsággal használjuk a számítógépet?
- hogyan illeszkedik az ütemezés a munkavégzési szokásainkhoz?

IRODALOMJEGYZÉK

FELHASZNÁLT IRODALOM

Könyvek

Kis Balázs Windows: XP haladó könyv második kiadás, SZAK Kiadó 2005

Kis Balázs – Szalay Márton: Windows Vista haladókönyv, SZAK Kiadó 2007

Hivatkozások

<http://www.kurt.hu> (2010-08-03)– adatmentés, adatbiztonság

<http://www.qnap.com> (2010-08-03)– NAS termékek gyártója

<http://wikipedia.hu> (2010-08-03) – Adattároló eszközök (ATA, SATA, Pendrive, NAS, RAID)

Windows XP Professional – Biztonsági másolat segédprogram súgója

AJÁNLOTT IRODALOM

Hivatkozások

<http://www.kurt.hu> (2010-08-03)– adatmentés, adatbiztonság

<http://www.qnap.com> (2010-08-03)– NAS termékek gyártója

<http://adatvedelem.lap.hu/> (2010-08-03) témához kapcsolódó linkgyűjtemény

A(z) 1174-06 modul 041-es szakmai tankönyvi tartalomeleme
felhasználható az alábbi szakképesítésekhez:

A szakképesítés OKJ azonosító száma:	A szakképesítés megnevezése
33 523 01 1000 00 00	Számítógép-szerelő, -karbantartó

A szakmai tankönyvi tartalomelem feldolgozásához ajánlott óraszám:
30 óra

MUNKANYAG

MUNKANYAG

A kiadvány az Új Magyarország Fejlesztési Terv
TÁMOP 2.2.1 08/1–2008–0002 „A képzés minőségének és tartalmának
fejlesztése” keretében készült.

A projekt az Európai Unió támogatásával, az Európai Szociális Alap
társfinanszírozásával valósul meg.

Kiadja a Nemzeti Szakképzési és Felnőttképzési Intézet
1085 Budapest, Baross u. 52.

Telefon: (1) 210–1065, Fax: (1) 210–1063

Felelős kiadó:
Nagy László főigazgató