HDS Check

A program célja, hogy az automatikus mentések során sérült adatok lehetőleg ne kerüljenek a mentésbe. Leginkább az átkódolós, zsarolós vírusok ellen próbál védelmet adni, így ennek bemutatásával készült az alábbi útmutató.

A Hard Disk Sentinel Pro (HDSP) beépített mentéses központot tartalmaz. A központ előre meghatározott műveleteket tud sorba rendezve indítani (másolás, külső program, stb...). A beépített másoló képes teljes, és különbözeti mentéseket készíteni. A mentések lehetnek "felülírásosak" (egy példányos mentés), és "körbeforgóak" (meghatározott időnként újabb mentés kerül dátumos könyvtár alá, és a legrégebbi ilyen törlésre kerül). A sorba rendezett mentések ha egymás utáni sorrendbe vannak felfűzve, csak akkor indulnak, ha az előző hibamentesen futott le. (Ez csak gyors emlékeztető, a pontos lehetőségeket a HDSP súgója tartalmazza.)

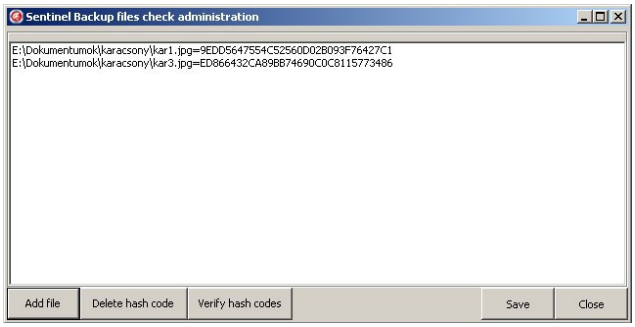
A kódolós vírusok jelenlegi változatai a gépet megtámadva, az összes betűjellel elérhető meghajtó dokumentumait erős titkosítással átkódolják. Így ez ellen védekezni csak megelőzéssel lehet. Legjobb, ha a fontos adatokról naprakész mentésünk van, sokszor automatikusra állítva. Ezzel csak az a baj, ha időben nem sikerül észlelni a vírust, a mentésünk is csak átkódolt adatokat fog tartalmazni.

A HDS Check segítséget nyújthat az automatikus felderítésben. Ehhez a mentendő adatok közé hasonló típusú ellenőrzésre használható állományokat kell tennünk (csali állományok). Ezek az állományok a későbbiekben NEM módosíthatóak! Megkülönböztetésükhöz azonos karakter sorozat adhat segítséget, mely a file nevében azonos helyen található. A kiterjesztés az eredeti tartalommal legyen összhangban. A HDS Check ezekről az állományokról ellenőrző kódot tárol, és azt ellenőrzi (ezért tilos módosítani). Ha hibátlanok, akkor sikeresen fut le, és nem ad hibaüzenetet, a mentés az adatokról elvégezhető. Ha viszont a vírus átkódolta a tartalmat, az ellenőrző kód megváltozik, és hibaüzenettel áll le. Így a HDSP-ben egymás utánra fűzött mentési modul már nem kerül indításra sem! Vagyis sérült adatok észlelése esetén a napi automatikus mentés blokkolásra kerül. Fontos tudni, hogy ez szúrópróba szerű ellenőrzés csak, így előfordulhat olyan állapot, mikor a vírus már aktív, folyamatosan kódol, viszont a kijelölt állományok tiszták még. Ilyenkor sajnos sérült mentés készülhet!

A fenti mentéses rendszert minimum 2 számítógépes hálózat esetén lehet felépíteni. Az optimális a 3 vagy több gép használata, ahol 2 szerver fut folyamatosan. Az egyik a munka szerver, a másik csak a mentéseket végzi. Az alábbi felsorolásban a HDS Check telepítésének és üzembe helyezésének folyamata olvasható:

1. A mentő szerverre kell telepíteni a HDSP-t és a HDS Check programot.
2. A munka szerveren a mentendő könyvtárakba kell helyezni az ellenőrzéshez használatos adatokat. Lehetőleg minél több könyvtárba kerüljön ellenőrző állomány, de túlzásba sem érdemes vinni.
3. A HDS Check program kiválasztó moduljával hálózati elérésen keresztül (NEM csatlakoztatott drive-ként!) ki kell választani a teszt állományokat, és az ellenőrző kódot el kell készíttetni vele.
4. A HDSP mentő központjában létre kell hozni egy külső programot indító project-et. Pl.:
   "C:\Program Files\Hard Disk Sentinel\CHK\SeFilesCheck.exe"
   Az ellenőrző programnak van két paramétere:
   -off : nem ír semmit a képernyőre (kikapcsolt vagy nem létező monitorra minek írjon)
   -r 3 : mennyi file-nak írja át az utolsó módosítás dátumát (random) a default=2
   itt a random miatt előfordulhat, hogy többször ugyan azt a file-t veszi elő tehát ez az érték inkább maximumnak felel meg. A file-ok használatát szimulálja, ne lehessen fix dátum alapján a csalit azonosítani.
   pl: "SeFilesCheck –off –r 5" vagy "SeFilesCheck –off"
5. A mentések kialakítás HDSP-n belül, a napi feladatoknál első lefutásúnak beállítva a Check modult. Célszerű az utolsó lefutó project-ben beállítani a mindenkori státusz e-mail küldését. A napi megjövő mail a rendszer és a levelezés működőképességét is visszajelzi! Vagyis nem felesleges szemét az a levél!

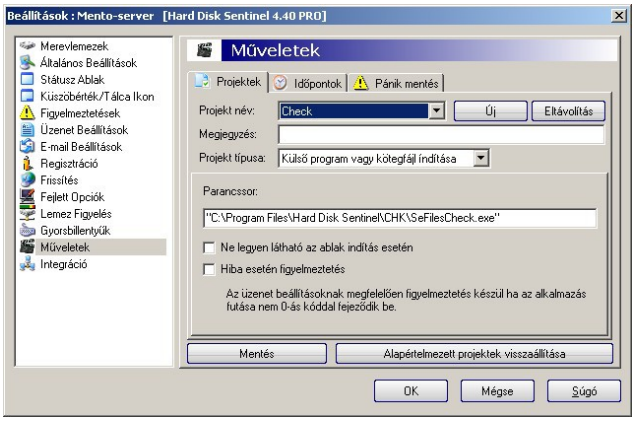
Képek a HDS Check beállításáról



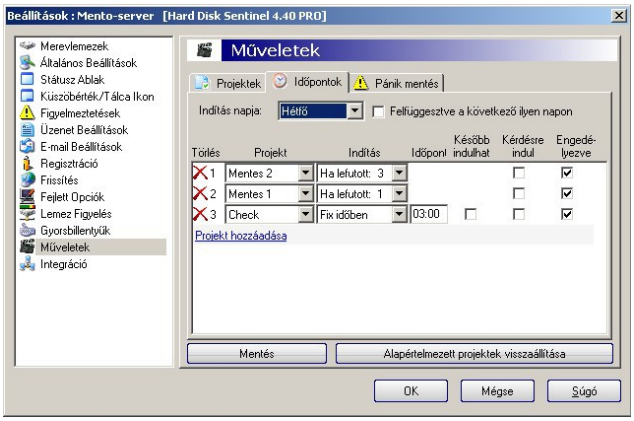
Kiválasztó program
(SeFilesCheckAdm.exe)

Add file:	file hozzáadása a listához
Delete hash code:	kiválasztott file törlése a listából
Verify hash code:	mentett kódok kézi ellenőrzése
Save:	összeállítás mentése file-ba
Close:	program bezárása

A programban menü segíti a file kiválasztását.

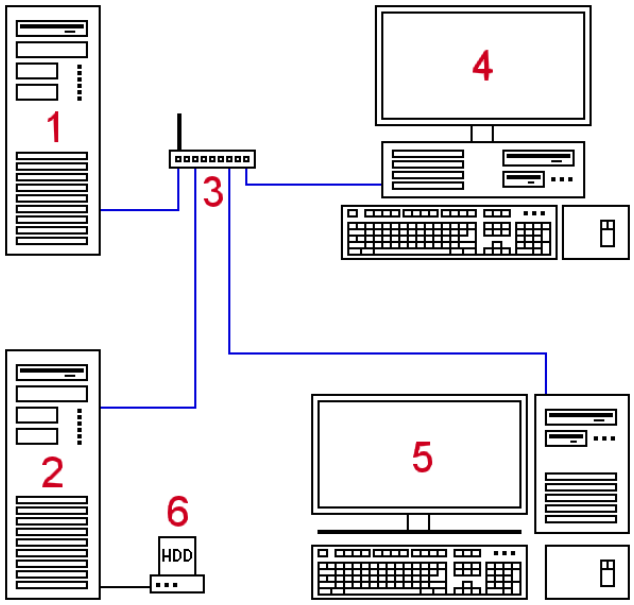


HDS Check project



Sorba állítás (a HDS Check utólagos beállításával)

Ideális kisvállalati környezet:



1. Központi (munka) szerver HDS és lehetőleg RAID1 (tükör) védelemmel ellátva. Teljesítménye a kívánt alkalmazásokhoz igazítandó.

2. Mentő szerver HDSP és HDS Check védelemmel.
Az 1-es szerverhez NINCS mount szintű kapcsolata. Alacsony fogyasztású integrált processzoros alaplap üzemeltetéséhez elegendő.

3. Switch esetleg router WiFi lehetőséggel.

4. Munkaállomás. Az 1-es szerverhez csak a nélkülözhetetlen drive mount engedélyezett.

5. Munkaállomás. (Mint a 4-es.)

6. HDD dokkoló. Az off-line mentések készítéséhez ideális.

Végül még egy pár ötlet. A mentéseket célszerű üres időszakra időzíteni, jellemzően hajnalra. Mivel kódolós vírus dolgozhat mentés időtartama alatt is, így csak a "körbeforgó" minimum 2 példányos mentés használata az ajánlott. A HDSP először törli a régebbi mentést, és utána hozza létre az új kópiát. Ha 2 példányos mentést kérünk, akkor meghagyja a tegnapit, és menti a mait (esetleg részlegesen kódoltat). Holnapra a vírus elvégzi dolgát, így a HDS Check észleli, és tiltja a mentés lefutását. Eredményként megmarad a tegnapelőtti hibátlan mentés. Ami viszont nem a "kellemetlen lenne elveszíteni", hanem az "életveszélyes" kategóriájú adatokat illeti, ott célszerű 3-5 példányos mentést beállítani. A dokkoló fontos része a mentő szervernek, hiszen az off-line mentéseket (dobozban a fiókban) itt lehet a legegyszerűbben, a napi munkát nem akadályozva elkészíteni. Ez is fontos része az egésznek! A kér szerver és a teljes automatikus rendszer ugyanis csak a működési biztonságot növeli, és előkészíti az adatbiztonságot. A dokkolóban készülő másolatok fizikailag is másik telephelyen tárolandóak. Ebben az esetben lesznek csak az adatok betörés, vagy természeti katasztrófa esetén is biztonságban.

Van még egy fontos szempont. A mentés tervezése azzal kezdődik, hogy mekkora az elviselhető adatvesztés mértéke az üzemeltető számára. Ennek ismeretében kell kialakítani a mentés rendszerességét (az on-line és off-line mentését is!).

Köszönet Reiter Tibornak, aki a HDS Check programot készítette az Interface Kft.-nél.