

Adatvédelmi és Adatmentési „Biblia”

Otthoni felhasználók számára

Írta: Vidi Rita

2009

Előszövegek

Amikor annak idején elterveztem, hogy na, most aztán rendbe teszem az otthoni felhasználók adatvédelmét, és készítek egy mit-és-hogyan anyagot, akkor valahogy az volt a fejemben, hogy egy fajsúlyos, komoly, nagyon átfogó ismeretsomagra van szükség.

Aztán, mikor elkezdtem a vázlatot készíteni, valahogy nem akaródzott nekifognom a megírásnak, összeállításnak. Lehet, hogy furán fog festeni, de bevallom: két napig gubbasztottam a vázlat fölött, és nem fogtam bele az írásba. Már az járt a fejemben, hogy lehetséges, hogy hirtelen kiszereztem a témából? Lehetséges, hogy meguntam, belefásultam? Lehet, hogy valami másra vágyom?

Ahhoz a praktikához folyamodtam, hogy itt hagytam a megnyitott vázlatot a gépen, hogy még véletlenül se felejtődjön el, hogy éppen mi a beütemezett feladatomban, ugyanakkor a gépet pedig csak kerülgettem naphosszat, és szívesebben foglalkoztam bármi mással :).

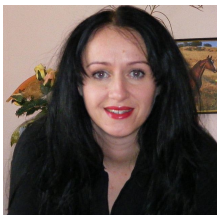
Éppen egy új mellényt kötöttem az ölembe pottyant „kényszerszabadidőmben”, amikor két sima és egy fordított szem között bevillant, hogy mi az, ami taszít az adat- és információvédelemről szóló anyagom elkészítésében: a hibás koncepció.

Ugyanis miért kéne ennek fajsúlyosnak, komolynak, mindent átfogónak és felölelőnek lennie? Hiszen én magam, aki annyi mindent tudok az adatvédelemről, és nyugodtan mondhatom magamról, hogy az adatvédelem mellett kardoskodó harcos amazon is vagyok egyben, én magam sem viszek túlzásba semmit, nem ragaszkodom rögeszmésen a túlszabályozáshoz, nem mentem kényszeresen az adatokat.

Éppen, hogy nem a komoly, fajsúlyos, száraz, tömör anyagokra van szükség, hanem ellenkezőleg: könnyed, betartható, elérhető, egyszerűen kivitelezhető technikákra és hogyanokra, mellé persze a szükséges elméletre.

Így született meg ez az anyag, így lett egyszerű, könnyű, ugyanakkor hasznos. Ja, és persze kötelező!
Fogyaszd egészséggel!

Vidi Rita



Felvezető kör

Azt hiszem, nem kell vitanapot indítanom arról, hogy az adatokat, az információt, a tartalmat védeni kell. Védeni, óvni, vigyázni rá, két nagyon fontos ok miatt:

1. Ha elvesz, nagyon gyorsan kiderülhet róla, hogy pótolhatatlan, és ez magával vonz rengeteg fejfájást, gondot, problémát, anyagi veszteséget.
2. Vannak olyan speciális adatok, amiknek a védelmét, megfelelő kezelését törvény írja elő. Ez természetesen otthoni felhasználókra kevésbé jellemző, de a teljes képhez ez is hozzátartozik.

A törvénnyel sosem szerencsés packázni - még a logikátlan, ellentmondásos törvényekkel sem -, ugyanakkor gyanítom, az **első pontot sem kell magyaráznom**. Nekem például, mint online vállalkozóknak, sorra kerülnek ki a kezeim közül az újabbnál újabb tartalmak, dokumentumok. Ezek számomra ugyanolyan értékkel bírnak, mint bármilyen iparágban az előállított termékek, vevőknek nyújtott szolgáltatások. Forintosítható, számszerűsíthető értékkel bíró adatok, információk ezek, amiknek az értéke igazából akkor tudatosodik bennünk, amikor elvesznek.

Sosem veszítettem fontos adatokat. Sosem veszítettem pótolhatatlan adatokat. De sírt már könyvelő a telefonomba, mert megsemmisültek az adatai, és kétségbe volt esve, mert éppen valami bevallás közeledett.

Láttam már sápadtan idegeskedni orvost, egy balul sikerült Linux telepítés után, mert véletlenül leformázta a teljes winchestert, és odalett hirtelen rengeteg, egy évtized orvosi praxisa alatt felgyűlt nagyon fontos - és törvényi szabályozás szerint kiemelten védett - adat.

Ezek csak a jéghegy csúcsai, nem akarlak efféle történetekkel fárasztani, és különben is, sose legyél ilyesminek se elszenvetője, de ha lehet, még tanúja se. Igazából szeretnék a megelőzésre és a pozitív hozzáállásra koncentrálni, de tény: sokkal több adat vész oda, mint bárki gondolná.

Az alábbiakban kitérünk arra,

- hogy mikor, miért, és hogyan kell adatot menteni,
- mit érdemes és mit KELL szabályozni
- kikkel kell önmagadon kívül elfogadtatni azt, hogy az adatokat pótolhatatlan kincsként kell kezelni,
- kapsz egy mintaszabályzatot, amit saját vállalkozásodra formálva aláírhatod és kirakhatod a falra
- és arról is szó lesz, hogyan kell eljárni katasztrófa helyzet esetén.

Az adatmentés kiskatéja

Gyorsan, már a legelején leszögezem, hogy tévedés azt hinni, hogy minél gyakrabban mentünk adatot, annál jobb. Ez csak a látszat. Adatot menteni optimális időközönként kell, de nem a gyakoriságon van a hangsúly, hanem azon, hogy MIT mentesz, hova, hány példányban, és hol, meddig tárolod.

Teszem azt, van a számítógépeden most per pillanat 55 GB adat. Hát, ezt naponta menteni elég macerás, gyakorlatban kivitelezhetetlen lenne. Ráadásul az 55 GB adat körülbelül darabszámra 1-2 milliónyi fájlt is jelenthet, amik fontossága igencsak különbözhet egymástól.

Ráadásul az adatmentés gyakoriságára egyéb más tényezők is jócskán hatnak, hogy ne menjek messzire a saját területemtől, például nem mindegy, hogy az adott gép, rendszer, vírusvédelmi szintje milyen színvonalú. Ha ócska, urambocsá gagyi, akkor a napi teljes körű adatmentés is kevés lehet, hiszen nagy a valószínűsége, hogy az adatmentéssel együtt a kártevőket is elmentenénk...

Őszinte leszek: ez az anyag önmagában, bármennyire is átfogó, lehet, hogy még kevés lesz a tökéletességhez. Viszont, ha ezt az anyagot kiegészíted a **10 Holtbiztos tippel**<<, akkor garanciát vállalok arra, hogy soha az életben nem fognak adataid véglegesen odaveszni. Fogadsz velem? Meg kell mondanom: csak így kerek a kép. Az adatok biztonságára nagyon sok minden hat, ennek egy része a vírusvédelem tökélyre fejlesztése. De csak egy része! A továbbiakban a többről lesz szó.

A biztonságos környezet mellett fontos adalékok szerepelnek az adatvédelem hatékonyságát tekintve:

1. Hardverek állapota - kiemelt fontosságú(ak) a merevlemez(ek)
2. Felhasználói készségek (ezen dolgozunk már egy ideje, igaz? :))
3. Szabályszerűség, ésszerűség, sőt egyszerűség
4. Szabályok betartása, betartatása
5. Külső segédeszközök igénybe vétele

Hardverek állapota, minősége

Már megint utálni fognak páran, de igen, létezik olyan winchester márka, amit még ellenségeimnek sem ajánlanék - na jó, nekik igen :) - ez a márka pedig a Samsung. Árban ugyanott van, mint az összes többi, meg ismerősnek tűnhet, mert ugyebár minden elektronikai eszközt le tudnak gyártani akár fejből is, de eddig az összes hardveres meghibásodás miatti adatvesztést Samsung winchester okozta a praxisunkban! Mi ilyen márkát nem is tartunk.

Természetesen egyetlen winchester sem örök életű, de a végleges meghibásodások előtt általában mindig vannak tünetek, viszont egyik pillanatról a másikra csak a Samsung szokott - rendszeresen - elszállni. Ez nem ijesztgetés, ezek tények a gyakorlatból. (Persze nem kell nekem hinni, de én előre szóltam!)

Az idők folyamán bármilyen gyártmányú winchestert utolérhet a végzete, bizonyos jelek utalhatnak erre:

- Az elhasználódás legenyhébb tünete a zaj. Vannak márkák, amelyekre kimondottan jellemző, hogy pár hónap után egyre hangosabbá válnak. Ez még önmagában nem gond, de már figyelmet érdemel, és készenlétet.
- Sokkal nagyobb baj, amikor az operációs rendszer egyszer csak elkezd NEM érzékelni a winchestert, majd mondjuk következő újraindulásnál megint „látja”. Egy otthoni felhasználónál még azt mondom ekkor, hogy nyugalom, egy-két alkalom nem a világ, de vállalkozóknál már inkább azt mondom, hogy: irány a bolt és új winchestert kell venni! Ha egyszer előfordul a kimaradás, akkor onnantól kezdve bármikor előfordulhat, ami a munkát tekintve enyhén szólva bosszantó lehet. Ilyenkor valószínűleg a merevlemez elektronikája kezdi megadni magát.
- A hardveres meghibásodásokból eredő adatvesztés harmadik leggyakoribb okozója a Megelőző Karbantartás című anyagban tárgyalt KOSZ! Erre nem térek ki bővebben most, nézd vissza azt az anyagot! *(Ez az anyag csak a rizsanélkül.hu oldalon vásárlóknak hozzáférhető - a szerk.)*

Felhasználói készségek

Bár az alcím azt sejteti, hogy minél tapasztaltabb valaki, annál kisebb a valószínűsége az adatvesztésnek, én itt is cáfolnám az összefüggést. Eleve a tapasztalat kifejezés nincs normálisan definiálva: ha valaki évek óta használja a gépet, kvázi **profinak hiszi magát, attól még nem az**. Minél többet foglalkozom felhasználók fejlesztésével, annál inkább érzem a szervezett oktatás szükségességét, szem előtt tartva az egyén fejlődésének dinamizmusát, és a kellő motiváltságot a megfelelő irányba való fejlődésre.

Mai napig ledöbbenek olyankor, mikor valaki már szinte warez-atyaúristenként tevékenykedik a neten, de a legapróbb kis vírusfertőzésnél már meg van löve.

Úgyhogy a tapasztalatot úgy fogalmaznám meg, hogy nem az a tapasztalt felhasználó, aki régóta és sok mindenre használja a gépét, hanem **az a tapasztalt felhasználó, aki a felbukkanó problémákat meg tudja oldani egyedül**. Persze nem lehet mindenki szakképzett szervizes és informatikus egy személyben, de a problémamegoldási készséget lehet fejleszteni.

Első lépése ennek, hogy érzékenyvé válunk a problémákra, vagyis amikor apró hibajelenséget tapasztalunk, akkor nem válunk vakká és süketté iránta, hanem egyből mérlegelünk, hogy közbe kell-e avatkozni, vagy analizálni kell, hogy mi okozhatta a problémát, és ez alapján kell-e vele foglalkozni... Tehát kulcsfontosságú az odafigyelés.

Mielőtt még hanyatt-homlok menekülnél, merthogy nem értesz a számítógéphez, problémákat meg pláne nem tudsz megoldani, gyorsan közlöm, hogy a **számítástechnika egyik legeslegnagyobb előnye az, hogy logikus...** Nagyon ritkák az ellentmondásos, ok nélküli esetek, minden összefügg, ok és okozat törvénye nem is lehetne szemléletesebb, mint ezen a területen.

A másik, amit gyorsan közlök: **ha megtanulsz egy problémát felismerni, akkor legközelebb már csukott szemmel is felismered**, és minél több ilyen irányú tapasztalatot szerzel, annál ügyesebb és magabiztosabb leszel, ráadásul a megelőző képességed is fejlődik. Ez nem egy hátrányos dolog, ha jól belegondolsz!

Tudom, hogy most valószínűleg nagyon intenzív fejlődési szakaszban vagy, és a hátad közepére sem kívánod a számítógépes problémákat, még tanulást segítő cézzal sem, ugyanakkor **ennek tudatában kell lenned, mert ez így működik.** A probléma megoldásban és felismerésben öntudatlanul is fejlődni fogsz, ezt megígérem. Ne görcsölj ezen, menni fog!

Jöjjön a dolog kellemetlenebbik része, amit nem lehet kiiktatni, nem lehet megkerülni, nem lehet megfélekezni róla:

Szabályszerűség, ésszerűség, sőt, egyszerűség

Ami nélkül nem működik az adatmentés és a megfelelő adat- és információvédelem, az a szabályszerűség. Mielőtt kiverne a víz már a szabályozás gondolatától is, tájékoztatlak, hogy a szabályszerűségnek van egy óriási előnye: kellőképpen kidolgozott formába rendezve nem kell többé magyarázni sem a gyerekeidnek, sem a szüleidnek, hogy mit vársz el adatvédelem terén a saját, nagyon szeretett számítógépeden, egyszerűen csak az orruk alá kell dugni a szabályokat, és esetleg még alá is lehet íratni velük, hogy tudomásul vették!

Nem, ez nem megkerülhető, ez kötelező! Gondolj csak bele, immár 6 oldalon keresztül magyarázom és fogadtatom el Veled, hogy az adatvédelem mennyire fontos, és mennyi minden hat rá. Gondolod, hogy neked könnyebb dolgod lenne a körülötted lévőkkel? Kétlem. Egészen biztos vagyok benne, hogy leírt, logikus szabályok nélkül egyszerűen a nullával egyenlő az adatvédelem szintje.

Nem kell semmit túlbonyolítani, nem kell túlzott fontosságot tulajdonítani neki, de szabályozni kell és a szabályokat alkalmazni kell. Ilyen egyszerű.

A szabályok és betartásuk garantálja, hogy:

1. Szinte nullára redukálódik az adatvesztés előfordulásának lehetősége.
2. Katasztrófa esetén nem tetéződik a baj, hanem megfelelően eljárva, azonnal a megoldáson lehet dolgozni, természetesen szervezett keretek között.

A második pont, úgy érzem, magyarázatra szorul. Egy példán keresztül mutatom be: teszem azt, hallasz arról, hogy rozsdás késsel az ujjunkat elvágni, nem egy kellemes esemény, sőt, hallasz elrettentő esetekről is, amikor egy ilyen ujjelvágás később teljes ujjvesztéshez vezetett. Úgy döntesz, hogy mindent megteszel a megelőzés érdekében. Ám minden óvintézkedés ellenére mégis megtörténik, rajtad kívülálló okok miatt - mondjuk nem kés, hanem egy lemezdarab vágja el az ujjadat. Az eredmény ugyanaz.

Nos, ha mégis megtörténik a baj, akkor mi a helyes cselekedet? Önmagadat próbálsz orvosolni, és az ismerősök elmondásai alapján jársz el, mondjuk paradicsomot meg efféle házi praktikákat vetsz be? Vagy elmész az orvoshoz, kitisztíttatod és bekötteted a sebet? Melyiknél nagyobb az esélye a felülfertőzésnek?

Sikerült rávilágítanom a mondanivalóm lényegére? **Baj esetén** nem sápítózni kell, vagy ismerősök tanácsára botorságokat csinálni, **hanem megfelelően kell reagálni**. Erre később visszatérünk, de amiért most itt szóba került, az az, hogy a reakciót, a megoldást is szabályozni kell, sőt még az is kiderülhet, hogy a problémás esetekben való eljárás szabályozása sokkal fontosabb lehet, mint a megelőzést biztosító szabályozás. Majd meglátjuk a tanulmány végén :).

Joggal merülhet fel benned a kérdés: „**Ha egyedül használom a gépemet**, akkor is leírt szabályokra van szükség? Nem elég, ha csak eldöntöm, hogy mi lesz?”.

Bár a gondolatoknak teremtő erejük van, de a tapasztalatom szerint az adatvédelem és az adatvédelmi szabályzat kérdéskörére nem gondolunk annyit, mint bármilyen vágyunkra, ezáltal a gondolat teremtő ereje is kevésbé érvényesül. Jobb egy fokkal, ha kimondunk dolgokat, de amikor magunkban beszélünk, az kissé furán veszi ki magát :).

Nézd: a legegyszerűbb leírni, kitenni valami szemmel látható helyre, és aztán azt a pár pontot következetesen betartani. Sokkal egyszerűbb ez a módszer, mint állandóan a fejben tartani valamit. Mikor már a gyakorlati kivitelezésnél fogunk tartani, látni fogod, hogy semmi extra nem lesz az adatmentési szabályzatban, tulajdonképpen egy frappáns kis csekklistád lesz.

Játékszabályok, amik a megelőzést szolgálják

Nem fogok visszamenni Ádámgig és Éváig a magyarázatban, a dolgok mozgatórugóinak utána lehet nézni a **10 Holtbiztos tipp** című anyagban. Álljon itt egy felsorolás, egy csekklista, az adatvédelem alapvető elveiről:

1. Tökéletes vírusvédelmi szint elérése, amely magában foglalja:

- legális, automatikus frissítésekre jogosult operációs rendszert,
- vírusirtót,
- tűzfalat,
- spam-ek elleni védelmet,
- az adatok mentési helyének tudatos megválasztását - nem az alapértelmezett Documents and Settings mappába!
- MSN használatának kiiktatását
- rendszeres adatmentést
- botnet rendszerbe való bekerülés megakadályozását
- a megfelelő böngésző megválasztását, a megfelelő biztonsági kiegészítővel (Firefox+Noscript kiegészítő)
- a helyi hálózatok biztonságát (semmit nem osztunk meg a hálózaton)

2. Megfelelő fizikai környezet a számítógép és az adattároló eszközök számára:

- Tűzbiztos környezet (nem dohányzunk, nem rakunk tüzet, az elektromos berendezések pedig nem működnek hibásan, a bútorzat nehezen éghető anyagból készül)
- Vízkár elleni védelem céljából érdemes minimum 1 méter magasságban tartani a számítógép házat, a padlótól számítva
- Rendszeres belső takarítás a számítógép házon belül - ha asztali gépről beszélünk, laptop esetén szakember segítségének igénybe vétele.

3. Hordozható eszközök kezelése:

- Pendrive, SD kártya, mp3 lejátszó használata kerülendő
- Elkerülhetetlen használat esetén - például nagyon gyors mentésre van szükség, és csak egy pendrive van kéznél - nem hurcoljuk magunkkal a mentett adatokat, mert óriási az elvesztés lehetősége.
- Más USB-s eszközt tilos rádugni a gépre - kivéve, ha ott áll melletted egy vírusvédelmi szakember -, és Te sem dughatod a sajátodat más gépére.

4. Egyéb biztonsági eszközök használata:

- Szünetmentes tápegység,
- Zavarszűrős elosztó

Ezek szolgálják a megelőzést. Ha a fentiek mind rendben vannak, akkor

- vírusok nem tehetnek kárt az adatokban,
- kémprogramok nem lophatják el a fontos adataidat,
- elemi kár, tűzkár-vízkár esetén kisebb a valószínűsége, hogy helyrehozhatatlanul megsérülnek az adatok,
- a ténylegesen hordozható adathordozókból eredő veszélyeket a nullára lehet redukálni - egyszerűen nem kell használni és kész, bármennyire trendi meg divatos, meg praktikus. Nekem nincs pendrive-om. Nekem, aki használom és tanítom is a számítástechnikát. Nem kell bedőlni minden újdonságnak, mert ezek fokozzák a veszélyeket (főleg, hogy belekeveredik az emberi tényező is). Ha más sem használhat a gépeden pendriveot, akkor nem fenyeget a mostanság olyan nagyon terjedő autorun kártevő.
- Hirtelen áramszünet esetén sem vesznek el az el nem mentett adatok.

Ezek csak az alapok. **Az igazán nagy dobás az adatvédelemben a rendszeres adatmentés.** Ugyanis, ha egy szerencsétlen pechsorozat folytán előfordul mégiscsak, hogy mondjuk betámadja a gépedet egy adattitkosító és kártérítést követelő vírus, akkor a kártevő leirtása után nevensz egyet a markodba, és visszatöltöd az adataidat a gépre. Nesze neked kártevő!

Ha teszem azt, épp egy árvízzel fenyegetett településen laksz, és egy éjjel arra ébredsz, hogy elöntötte a házatokat a víz bokáig - Isten ments, hogy ez bárkivel előforduljon! De az ördög nem alszik... - és menekülni kell, és van rendszeres adatmentésed, a szekrény tetején egy zárható kazettában, akkor egy fokkal nyugodtabb lehetsz, de akár még az is előfordulhat, hogy az elázott számítógépről is vissza lehet menteni az adatokat.

A Te dolgod az, hogy a veszteség kockázatát redukáld. Ha nem teszed meg, akkor bevonzod a bajt egyrészt, másrészt pedig csak a vak szerencse vezérli az életedet.

Mit mentsek?

Kezdjük ott, hogy az adatokat menedzselni kell. Nem lehet mindent egy kupacba ömlesztetni, szét kell válogatni, tudni kell, hogy mi a munka, és mi a szórakozás, mi a nagyon fontos, és mi a kevésbé.

Első lépésként hozz létre egy [fontos] nevezetű könyvtárt, és ebben, alkönyvtárakba csoportosítva gyűjtsd össze a fontos, családi, személyes, vagy munkához szükséges, céget, vállalkozást érintő adatokat. Ha használod már egy ideje a gépet, és mondjuk rendszeresen fényképezel, vagy dokumentumokat állítasz elő, itt össze tud gyűlni pár gigabájtnyi adat.

És most jön a jó hír: **ezt a könyvtárat kell rendszeresen mentened.**

Első szabály: Mentsd rendszeresen a fontos adataidat. Mitől fontos egy adat? Például attól, hogy sok időbe kerül előállítani. Például hetekig küzdesz a blogod bejegyzéseinek előállításával? És csak fenn az oldalon vannak meg? Óreg hiba!

Vagy teszem azt, hetek óta írod a szakdolgozatodat, már készen van 75 oldal, és csak a számítógépeden tárolod? Csoda, hogy még megvan!

Esetleg napokig tervezted és szerkesztetted a főnökség előtt bemutatandó prezentációd, és nincs belőle biztonsági másolatod?

Azokat az adatokat mentsd, amik előállítására sok időt és energiát fordítottál, és újabb napokba, hetekbe, hónapokba telne előállítani.

Nézd úgy az adataidat, hogy: **„Ha ez elveszne, napokra letargiába kerülnék?” Ha igen a válasz, akkor mentés!**

Netről bármikor letölthető, kismilliónyi adatot nem kell állandóan DVD-re írogatni, mert azt bármikor lemented újra, vagy elkéred valakitől. Ez vonatkozik zenékre, filmekre, letöltött képekre.

Második szabály: mentsd azokat az adatokat, amik **az életed részei**. Családi fényképek, videók. (Ezeket szokták a legjobban bánni az adatvesztéskor, illetve a hosszú ideje készülő információs termékeket, szakdolgozatokat, írásokat.)

Harmadik szabály: mentsd azokat az adatokat, amik külső forrásból származó, de nem pótolható adatok. Tehát **a levelek**. Ez a legegyszerűbb: használj levelező klienst, vagyis töltsd le a gépedre a leveleket, ugyanakkor hagyd meg a levelező tárhelyeden is az eredeti példányokat. Ezt a levelező kliens - Thunderbird, Outlook - beállításának egy kis pipával be lehet iktatni, onnantól kezdve az elveszett levelek problémája örökre ki van iktatva. A továbbiakban már csak az általad küldött levelek mentésére kell figyelned, hiszen ezek nem kerülnek fel a tárhelyre, ha a klienssel írod és küldöd. Visszatekintve az elmúlt két évemre, körülbelül kettő általam elküldött levelet kellett visszakeresnem, és persze megvoltak, mert minden kimenő levelet tárolok.

A levelező kliensek egy általuk létrehozott mappában tárolják a leveleket, és **itt van egy nagy veszélye az Outlooknak:** 2 GB-nál nem képes nagyobb mappát kezelni, tehát ha az egész mappa eléri ezt a határt, akkor eltűnnek a levelek. (Ezért is jobb a Thunderbird.)

Én nem tartom helyénvalónak az ész nélküli adattárolást. 100 levélből átlagban 5-re lesz szükség 1 hónap eltelte után, ami azt jelenti, hogy 95%-a a leveleknek csak a helyet foglalja. Tudnod kell szelektálni, és tartanod kell egy határt.

Egyébként ebbe nem akarok beleszólni, azt használj, amit akarsz - ez egy állandó vitaforrás, hogy ki milyen szolgáltatót és milyen klienst tart megfelelőnek -, ez a szubjektív megítélés területe alá esik, nekem mindegy. De vigyázz a leveleidre külön is! Ebbe beleszóllok :).

Tükrözzünk vagy ne tükrözzünk?

Minden felhasználónak felcsillan a szeme, amikor először hall a RAID, vagyis adattükrözés lehetőségéről. A gyakorlatban úgy néz ki, hogy a rendszer tulajdonképpen egyszerre két merevlemezt használ, az egyik a másiknak azonnali biztonsági másolata tulajdonképpen. Nap végén egyszerűen csak az egyiket ki kell venni, el kell zárni, és kész, le van tudva az adatmentés.

Igen, ez így szépen hangzik, de csak hangzik. Kapásból nem mindegy, milyen operációs rendszerünk van. Kapásból nem mindegy, milyen két merevlemezezt beszélünk. Az sem mindegy, egyébként mekkora szuflával bír a gépünk, hiszen egyszerre két merevlemezt kell hajtania (és azok dolgoznak is szépen ám!), és milyen plusz erőforrásokat igényel a tükrözés folyamata.

Aztán ott van a pakliban az is, hogy ha naponta 3 nagyon fontos fájl hozol létre, akkor minek akarod folyamatosan dolgoztatni és felügyelet alatt tartani a két merevlemezt teljes egészében? A RAID technológia nem bonyolult, de amint használatba kerül, az még egy szög a hatékony számítógép felhasználás koporsójába. Ugyanis felügyeletet kíván (erre vannak a rendszergazdák többek között).

Igen, közép- és nagyvállalatoknál, amikor az emberi tényezőt egy bizonyos fokon túl már kénytelenek kiiktatni, akkor szükséges a RAID, de arra külön szerverek vannak igénybe véve, ami megint nem 10ezer forintos kategória.

Sokkal fontosabb, hogy használjuk az eszünket, ugyanakkor tartsuk be a megelőzési és szinten tartási szabályokat. Ennyi.

Hogyan mentünk adatot?

Na, ez a legérdekesebb és legizgalmasabb része a dolognak. **Az egész adatmentős dolog azért szokott megbicsaklani, mert muszáj, hogy egyéni legyen.** Ugyanakkor, ha egyéni, akkor meg már el is lehet sumákolni. Ezért most nem kötelezlek semmire, de javaslok két olyan módszert a CD és DVD írás mellett, ami tökéletesen beválik a otthon is.

Ez a két módszer majdnem ugyanaz: egy másik merevlemez hadrendbe állítása, vagy egy mobil - de a számítógép házba illeszthető - rack, vagy egy külső, USB-s ház segítségével. Ez utóbbi elterjedtebb és kedveltebb mostanság, ami nem csoda: annyira egyszerű a használata, hogy a 3 éves kisfiam is elboldogulna vele.

Mivel az általam preferált adatmentési szabályzat eleve adatmenedzselést feltételez - és igen, vesszek meg, ha leteszek arról, hogy szerintem fejleszteni kell a felhasználókat, nem pedig mindenféle hangzatos kütyüvel és hardverrel oldani meg a problémákat -, az adatmentés maga már pofon egyszerű: általad meghatározott időközönként a fontos

adatokat át kell másolni az adatmentésre - biztonsági másolatok tárolására - fenntartott merevlemezre.

Az első adatmentés lehet teljes körű, tehát a számítógépeden tárolt minden adatot átmásolsz a remélhetőleg hatalmas kapacitással rendelkező külső merevlemezre, például a dátumnak megfelelő mappába: [20090131] (ezen a napon mentetted mondjuk az adatokat). Ebbe bekerül minden adatod, könyvtárostól, alkönyvtárostól, fájlostól.

Ezek után a lehető leggyakrabban, amely gyakoriság még nem megy az agyadra, külön könyvtárba, szintén dátum szerint beazonosítva mentheted a fontos adatokat, amiket előtte persze menedzselteél, vagyis fontosnak tituláltál és egy helyre gyűjtöttél.

Pl. [mentes0201] [mentes0208] [mentes0215] és így tovább. Ebben az a szép, hogy amikor már a harmadik-negyedik mentést csinálod az egyre frissülő, fontos adatokat tartalmazó könyvtáradról, akkor **a régiéket, létrehozási sorrendben el lehet kezdeni törölni.** Vagyis nem kell örök időig tárolni az adatokat.

A példamban heti mentést irányoztam elő - ha észrevetted - és azt kell, hogy mondjam, ez a minimum időintervallum, amit be kell tartanod. Ennél több időt nem szabad hagyni két adatmentés között, kivéve, ha szabadságot magad egy hétre, és hozzá sem nyúlsz a gépedhez és nem hozol létre fontos, pótolhatatlan fájlokat.

Viszont most akkor álljunk meg egy pillanatra: tételezzük fel, hogy vállalkozó vagy - hobbifelhasználók bocsánat, sok vállalkozó olvassa az anyagot! - Te hetente egyszer szeretnél adatok mentésével foglalkozni. Szeretnéd, ha a neked dolgozó munkaerők is így járnának el? Szerintem nem. Úgy vélem, szeretnéd, ha minden nap mentésre kerülnének az adatok az alvállalkozók keze alatt. Nos, ha ezt megköveteled másoktól, akkor neked magadnak kell példát mutatnod, illetve kipróbálnod, hogy a gyakorlatban ez milyen erőforrásokat igényel.

Néhány megabájtnyi adat, napi szintű mentése külső merevlemezre, körülbelül 5 percet vesz igénybe:

1. A külső merevlemez az USB csatlakozóval a gépre dugjuk.
2. Merevlemez házán található kapcsolóval áramot biztosítunk a külső egység számára.
3. Total Commanderben - vagy bármilyen fájlkezelő klienssel - megnyitjuk a külső merevlemez gyökérkönyvtárát, létrehozunk egy aznapi mentésre utaló névvel ellátott könyvtárat, és bemásoljuk a mentendő adatokat.
4. Total Commandert bezárjuk.
5. Az óra melletti értesítési területen lévő, USB-s háttértárolók biztonságos eltávolítására szolgáló kis ikonra kattintunk, és eltávolítjuk az eszközt (külső meghajtó).
6. Ha kész a digitális eltávolítás, a külső házon lévő kapcsolóval

- megszüntetjük az áramellátást.
7. Kihúzzuk az USB aljzathoz.
 8. Biztos helyre tesszük.

A legtöbb időt az eszköz elővétele és elpakolása jelenti tulajdonképpen, és persze az adatmennyiségtől függően a másolás időtartama.

Ugye, hogy semmi extra nincs benne?

A külső merevlemez tároló mellett most kezd elterjedni a pénztárca méretű merevlemezek kora. Ezek laptopokba való merevlemezek, és kis tokban vannak. Olyan, mint egy kicsi határidő napló. A mérete megtévesztő, mert 250 GB adat is elférhet rajtuk. Ezek a kicsit drágább kategóriába tartoznak, de olyannyira diszkrétnek, és olyan kis helyet igényelnek, hogy érdemes megfontolni a beszerzését.

Western Digital
winchester
2.5” HDD (kicsi)



Jelszóval védhető
külső ház



Ha már a jelszóval levédhető külső merevlemez ház bekerült a képbe, térjünk ki egy kicsit az adatok titkosítására!

Titkosítási egyszeregy

Pofon egyszerű **titkosítási eljárást** fogok megmutatni, olyan egyszerű, hogy tulajdonképpen nem is értem, miért nincs elterjedve. Ez a módszer megnyitja az utat az FTP tárhelyeken való tárolás lehetősége előtt is, mert... Na figyelj, mutatom:

A legegyszerűbb és legolcsóbb titkosítási módszer, amit pillanatok alatt beüzemelhetsz minden egyes adatmentés előtt, ha a fájlokat, illetve a mentendő mappát tömörítve - becsomagolva - mented, és jelszóval védeted le. A titkosítás előtt lehet választani, hogy milyen erősségű titkosítást kérsz, és Te adod meg a jelszót, amit aztán kicsomagoláskor meg kell adni természetesen.

Total Commanderben jobb klikk a könyvtárra/fájltra, amit be akarsz csomagolni. Megjelenik az alapértelmezett tömörítő, és az általános opciókkal készen áll a becsomagolásra. Mielőtt még okét nyomnál, **pipáld be a Titkosítás opciót is**. Ekkor választhatsz, hogy milyen kódolással legyen titkosítva. Az AES256 kiváló lesz, még egy profi is hónapokat küzd vele, mire feltöri, ha elveszítened mondjuk a merevlemezedet, vagy urambocsá, a pendrive-odat.

Már itt meg kell adnod egy jelszót, illetve még egyszer meg kell erősítened a jelszót.

Amikor készen van a folyamat, megpróbálhatod megnyitni, kicsomagolni a tömörített fájlokat, de ekkor már jelszót kell beírnod. A nézőkével sem tudsz belepislogni (Total Commander F3), mert ahhoz is kéri a jelszót. Viszont törölni tudod a fájlt, tehát az ellen nem véd :).

Ha a becsomagolós-jelszavazós módszert választod, akkor azt javaslom, hogy a jelszavakat ne nagyon variáld meg, mert ha elfelejted, akkor te se fogod többé visszafejteni. Legyen egy alap jelszavad - benne nagy betűk is - és bizonyos karakterek változzanak titkosított fájlként.

Ennél bonyolultabb és minden egyes bájtot titkosító programra tulajdonképpen nincs szükség. Praktikus, gyorsan kezelhető, atombiztos.

Már tudjuk, hogyan lehet menteni, már tudjuk, mit kell menteni, azt is, milyen időközönként érdemes, mire, és kinek. Most már ideje, hogy szabályszerűsítsük.

Az alábbi szabályzat bármilyen kis vállalkozás számára szabadon felhasználható. (Otthoni felhasználók számára lásd a második szabályzatot.)

Szabályzat/1.

[CÉGNEVE] Adatvédelmi és Adatmentési Információbiztonsági Szabályzata

A szabályzat célja, hogy biztosítsa [CÉGNEVE] és alvállalkozói, alkalmazottai által kezelt adatok vonatkozásában az adatbiztonság követelményeinek érvényesülését. Megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

Az Adatvédelmi és Adatmentési és Információbiztonsági Szabályzat hatálya kiterjed a [CÉGNEVE] valamennyi szervezeti egységére – telephelytől függetlenül -, ahol a céggel kapcsolatos, vagy személyes, különleges vagy közérdekű adatokat kezelnek.

Az adatvédelmi felelős (ez vagy Te!)

- (1) Irányítja, felügyeli, ellenőrzi az adatvédelmi tevékenységet.
- (2) Ellenőrzi az Adatvédelmi és Adatmentési Szabályzat betartását
- (3) elkészíti és aktualizálja az Adatvédelmi és Adatmentési Szabályzatot;

Az adatkezelést végző személy (alvállalkozó, alkalmazott)

- (1) tevékenységi körén belül felelős az adatok feldolgozásáért, megváltoztatásáért, törléséért, továbbításáért és nyilvánosságra hozataláért
- (2) kezeli és megőrzi a feladata ellátása során birtokába került adatokat,
- (3) a kiadott adatmentési utasítás alapján rendszeresen adatmentést végez.
- (4) gondoskodik arról, hogy az általa vezetett nyilvántartások adataihoz illetéktelen személy ne férhessen hozzá,
- (5) betartja az adatkezelésre vonatkozó jogszabályokat és belső utasításokat,
- (6) részt vesz az adatkezeléssel, adatvédelemmel összefüggő szakmai képzéseken,

Az adatkezelés szabályai (figyelem, Adatvédelmi törvénynek megfelelő!)

Személyes adatok kezelése

- (1) Személyes adat a [CÉGNÉV] által akkor kezelhető, ha
 - ahhoz az érintett hozzájárul, vagy
 - valamely jogszabály elrendeli.
- (2) Az érintett az adatkezelőtől tájékoztatást kérhet személyes adatai kezeléséről, és az adatokba bele is tekinthet. A betekintést úgy kell biztosítani, hogy az érintett más személy adatait ne ismerhesse meg. (Atv.12, 13. §)
- (3) Az érintett kérelmére az adatkezelő tájékoztatást ad az általa kezelt adatairól, az adatkezelés céljáról, jogalapjáról, időtartamáról, továbbá arról, hogy kik és milyen célból kapták meg az adatokat.
- (4) Adat változás vagy téves adatrögzítés észlelése esetén az érintett írásban kérheti kezelt adatainak helyesbítését, illetve kijavítását. A téves adatot az adatkezelő 8 munkanapon belül helyesbíteni köteles. (Atv.15. §)
- (5) Személyes adatok akkor továbbíthatók, valamint különböző adatkezelések akkor kapcsolhatók össze, ha az érintett ahhoz hozzájárult, vagy azt törvény megengedi és ha az adatkezelés feltételei minden egyes személyes adatra nézve teljesülnek.
- (6) Olyan adatkezelés esetén, amelynél számolni kell külföldre irányuló

adattovábbítással, az érintettek figyelmét erre a körülményre már az adatok felvétele előtt fel kell hívni. Az érintett írásbeli felhatalmazása nélkül személyes adat külföldre nem továbbítható, kivéve, ha ezt törvény lehetővé teszi.

(7) A [CÉGNÉV] szervezetén belül a kezelt személyes adat - a feladat elvégzéséhez szükséges mértékben és ideig - csak az ügyvel érintett szervezeti egységhez továbbítható, feltéve, hogy a személyes adatok megismerése nélkül az ügyben érdemben eljárni nem lehet.

(8) A [CÉGNÉV] szervezetén belül a különböző célú adatkezelések csak törvényes cél érdekében, indokolt esetben, ideiglenesen kapcsolhatók össze.

(9) Az adatkezelések összekapcsolásával, valamint a megkeresés alapján teljesített adatszolgáltatással kapcsolatos alábbi tényeket, körülményeket jegyzőkönyvben kell rögzíteni:

- az adatkérő (az összekapcsolt adatkezelések) megnevezése;
- az adattovábbítás (összekapcsolás) célja, rendeltetése;
- a továbbított (összekapcsolt) adatok köre;
- az adattovábbítás (összekapcsolás) jogszabályi alapja;
- az adattovábbítás (összekapcsolás) módja.

(9) Nem kötelező adatszolgáltatáson alapuló adatkezelés esetén az érintett indokolás nélkül írásban kérheti kezelt adatainak törlését. A törlést 8 munkanapon belül el kell végezni.

(10) Az érintett az adatkezeléssel kapcsolatos jogainak megsértése esetén az illetékes szervezeti egység vezetőjéhez, illetve az adatvédelmi felelőshöz fordulhat.

(11) Ha az adatkezelést a [CÉGNÉV] szervezetén kívüli adatfeldolgozó végzi, akkor az adatfeldolgozásra az Avt 4/A.§ rendelkezései érvényesek.

Adatbiztonság

Az adatbiztonság általános szempontjai

(1) Az adatkezelő köteles gondoskodni az általa kezelt adatok biztonságáról.

(2) Az adatokat védeni kell a jogosulatlan hozzáférés, a megváltoztatás, a továbbítás, a nyilvánosságra hozatal, a törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen.

(3) Adatkarbantartást csak az erre felhatalmazott adatkezelő végezhet.

(4) A számítástechnikai rendszerek üzemeltetését ellátó munkatársak a feladataik ellátásához szükséges mértékig az adatállományokhoz hozzáférhetnek, az adatokat azonban más célra nem használhatják fel, és mások tudomására nem hozhatják.

Az adatok mentése, az adathordozók biztonsága

A napi adatmentés a következő módon történik

(1) Az adatvédelmi felelős által meghatározott fájlokat, naponta, a munka befejeztével AES-256 erősségű jelszóval védett .zip fájlba tömörítve az adatmentés helyének kijelölt külső merevlemezre kell másolni, az asznapi dátumra utaló megnevezéssel ellátott, új, erre a célra létrehozott könyvtárba.

(Vagy feltöltheti az erre a célra létrehozott FTP tárhelyre, ez a rész tetszőlegesen módosítható)

(2) A külső, biztonsági másolatokat tartalmazó merevlemezt csak az

adatmentés idejére szabad üzembe állítani, az adatmentés befejeztével szabály szerűen el kell távolítani a rendszerből, és az adatvédelmi felelős által kijelölt helyre kell elzárni. *(FTP tárhelyre való feltöltés esetén ez úgy módosul, hogy csak a feltöltés idejére szabad az FTP kapcsolatot élővé tenni, adatfeltöltés után a kapcsolatot meg kell szakítani.)*

(3) A korábbi adatmentéseket csak az adatvédelmi felelős írásbeli utasítására szabad törölni, általánosan a 14 napnál régebbi fájlok kerülhetnek törlésre, de csak abban az esetben, ha már létezik legalább 13, frissebb adatmentés az állományokról.

A heti adatmentés a következő módon történik

(1) Az adatvédelmi felelős által meghatározott, de általánosságban elmondható, hogy a merevlemezen lévő összes fájlról hetente egyszer teljes körű biztonsági másolatot kell készíteni. Az adathalmaz méretének megfelelően vagy a napi adatmentésnél már szokásos AES-256 erősségű jelszóval védett .zip fájlba tömörítve, vagy az eredeti állapotban; az adatmentés helyének kijelölt külső merevlemezre kell másolni, az aznapi dátumra utaló megnevezéssel ellátott, új, erre a célra létrehozott könyvtárba, a könyvtár nevében utalva arra, hogy heti és teljes körű, minden adatot érintő biztonsági másolatról van szó.

(2) A külső, biztonsági másolatokat tartalmazó merevlemez csak az adatmentés idejére szabad üzembe állítani, az adatmentés befejeztével szabály szerűen el kell távolítani a rendszerből, és az adatvédelmi felelős által kijelölt helyre kell elzárni. *(Ennél az esetről az óriási adathalmaz lehetősége igen nagy, tehát tárhelyre feltölteni nem szerencsés.)*

(3) A korábbi, heti, teljes körű adatmentéseket csak az adatvédelmi felelős írásbeli utasítására szabad törölni, általánosan az 1 hónapnál régebbi biztonsági mentést tartalmazó könyvtárak kerülhetnek törlésre, de csak abban az esetben, ha már létezik legalább 3 (három), frissebb adatmentés az állományokról.

Adatvesztés, elemi kár, bármilyen, adatokat érintő probléma esetén követendő eljárás

(1) Az adatkezelő munkatárs az adatok épségét, hozzáférhetetlenségét veszélyeztető legapróbb jelet észlelve köteles értesíteni az adatvédelmi felelőst.

(2) Az adatkezelő munkatárs a veszély legapróbb jelét észlelve azonnal abbahagyja a munkát, az elmentetlen dokumentumokat elmenti, és az adatvédelmi felelős további utasításáig nem nyúl sem a számítógéphez, sem a biztonsági másolatokat tartalmazó merevlemezhez.

(3) Az adatvédelmi felelős saját hatáskörében és az adatkezelő munkatárs jelzésére is dönthet úgy, hogy az adatok biztonságára nézve veszélyhelyzetnek értékeli a jeleket és tüneteket.

(4) Az adatvédelmi felelős haladéktalanul értesíti a [CÉGNÉV]-vel szerződésben álló szervizt/rendszergazdát.

(5) A szervizes/rendszergazda kéréséig az adatvédelmi felelős biztosítja az érintett számítástechnikai eszközök elkülönítését *(senki nem nyúlhat*

hozzá, még az adatvédelmi felelős sem)

Adatok visszatöltése, adatmentési pontok visszaállítása

A napi és heti rendszerességgel mentett adatokat csak az adatvédelmi felelős tudtával és írásbeli beleegyezésével szabad visszatölteni *(ugyanis tudnod kell, mi az oka! Csak úgy bele a vakvilágba nem tölthető vissza az adatok!)* Az adatok visszatöltéséről jegyzőkönyvet kell készíteni.

.....
Dátum

.....
Cégvezető/EV

Kellőképpen belezsibbadt már az agyad? (Egyébként elismerésem, ha végigolvastad!)

Otthoni felhasználók számára javasolt szabályzat:

Szabályzat/2.

Adatbiztonság

Az adatbiztonság általános szempontjai

- (1) Az adatkezelő köteles gondoskodni az általa kezelt adatok biztonságáról.
- (2) Az adatokat védeni kell a jogosulatlan hozzáférés, a megváltoztatás, a továbbítás, a nyilvánosságra hozatal, a törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen.
- (3) Adatkarbantartást csak az erre felhatalmazott adatkezelő végezhet.
- (5) A számítástechnikai rendszerek üzemeltetését ellátó munkatársak a feladataik ellátásához szükséges mértékig az adatállományokhoz hozzáférhetnek, az adatokat azonban más célra nem használhatják fel, és mások tudomására nem hozhatják.

Az adatok mentése, az adathordozók biztonsága

A napi adatmentés a következő módon történik

- (1) Az adatvédelmi felelős által meghatározott fájlokat, naponta, a munka befejeztével AES-256 erősségű jelszóval védett .zip fájlba tömörítve az adatmentés helyének kijelölt külső merevlemezre kell másolni, az aznapi dátumra utaló megnevezéssel ellátott, új, erre a célra létrehozott könyvtárba. *(Vagy feltöltheti az erre a célra létrehozott FTP tárhelyre, ez a rész tetszőlegesen módosítható)*
- (2) A külső, biztonsági másolatokat tartalmazó merevlemez csak az adatmentés idejére szabad üzembe állítani, az adatmentés befejeztével szabály szerűen el kell távolítani a rendszerből, és az adatvédelmi felelős által kijelölt helyre kell elzárni. *(FTP tárhelyre való feltöltés esetén ez úgy módosul, hogy csak a feltöltés idejére szabad az FTP kapcsolatot élővé tenni, adatfeltöltés után a kapcsolatot meg kell szakítani.)*
- (3) A korábbi adatmentéseket csak az adatvédelmi felelős írásbeli utasítására szabad törölni, általánosan a 14 napnál régebbi fájlok kerülhetnek törlésre, de csak abban az esetben, ha már létezik legalább 13, frissebb adatmentés az állományokról.

A heti adatmentés a következő módon történik

(1) Az adatvédelmi felelős által meghatározott, de általánosságban elmondható, hogy a merevlemezen lévő összes fájlról hetente egyszer teljes körű biztonsági másolatot kell készíteni. Az adathalmaz méretének megfelelően vagy a napi adatmentésnél már szokásos AES-256 erősségű jelszóval védett .zip fájlba tömörítve, vagy az eredeti állapotban; az adatmentés helyének kijelölt külső merevlemezre kell másolni, az aznapi dátumra utaló megnevezéssel ellátott, új, erre a célra létrehozott könyvtárba, a könyvtár nevében utalva arra, hogy heti és teljes körű, minden adatot érintő biztonsági másolatról van szó.

(2) A külső, biztonsági másolatokat tartalmazó merevlemez csak az adatmentés idejére szabad üzembe állítani, az adatmentés befejeztével szabály szerűen el kell távolítani a rendszerből, és az adatvédelmi felelős által kijelölt helyre kell elzárni. *(Ennél az esetről az óriási adathalmaz lehetősége igen nagy, tehát tárhelyre feltölteni nem szerencsés.)*

(3) A korábbi, heti, teljes körű adatmentéseket csak az adatvédelmi felelős írásbeli utasítására szabad törölni, általánosan az 1 hónapnál régebbi biztonsági mentést tartalmazó könyvtárak kerülhetnek törlésre, de csak abban az esetben, ha már létezik legalább 3 (három), frissebb adatmentés az állományokról.

Adatvesztés, elemi kár, bármilyen, adatokat érintő probléma esetén követendő eljárás

(1) Az adatkezelő munkatárs az adatok épségét, hozzáférhetetlenségét veszélyeztető legapróbb jelet észlelve köteles értesíteni az adatvédelmi felelőst.

(2) Az adatkezelő munkatárs a veszély legapróbb jelét észlelve azonnal abbahagyja a munkát, az elmentetlen dokumentumokat elmenti, és az adatvédelmi felelős további utasításáig nem nyúl sem a számítógéphez, sem a biztonsági másolatokat tartalmazó merevlemezhez.

(3) Az adatvédelmi felelős saját hatáskörében és az adatkezelő munkatárs jelzésére is dönthet úgy, hogy az adatok biztonságára nézve veszélyhelyzetnek értékeli a jeleket és tüneteket.

(4) Az adatvédelmi felelős haladéktalanul értesíti a [CÉGNÉV]-vel szerződésben álló szervizt/rendszergazdát.

(5) A szervizes/rendszergazda kéréséig az adatvédelmi felelős biztosítja az érintett számítástechnikai eszközök elkülönítését *(senki nem nyúlhat hozzá, még az adatvédelmi felelős sem)*

Adatok visszatöltése, adatmentési pontok visszaállítása

A napi és heti rendszerességgel mentett adatokat csak az adatvédelmi felelős tudtával és írásbeli beleegyezésével szabad visszatölteni *(ugyanis tudnod kell, mi az oka! Csak úgy bele a vakvilágba nem tölthetőek vissza az adatok!)* Az adatok visszatöltéséről jegyzőkönyvet kell készíteni.

Természetesen tudom, hogy otthoni felhasználóként most levegő után kapkodsz. Azt gondolod: *micsoda? Ilyen száraz szakszöveget kell bevezetnem otthon?*

Nem, nem KELL. Csak javasolt.

Fogalmazd át viccesre, vagy a stílusodnak megfelelőre, csak legyen értelme, és legyen meg a gyakorlati haszna.

Kiskapu: használd nyugodtan a Vírusvédelmi és Adatmentési naplót, amit innen tölthetsz le: <http://www.viruskommando.hu/titok/naplo.xls>

A napló, kellőképpen szem előtt tartva - pl. falra kirakva - tulajdonképpen mindig figyelmeztet az adatvédelem fontosságára, és nem utolsó sorban a víruskereséssel kapcsolatos rendszerre is.

Tudom, nagyon sokan a szabályozás szót is kiirtanák legszívesebben a szótárból, és ellene vannak minden előírásnak. A Te dolgod, ha így gondolod, én csak egyet kérdezek: **vezet AZ valahova?**

Azért, mert az általad ismert szabályok inkább gátoltak, mint segítettek, attól még lehet egy szabálynak értelme, és van is.

A felhasználók 95%-a még mindig abban az álomvilágban él, hogy a számítógép nem bonyolultabb egy mobiltelefonnál, és netezni éppen csak annyit jelent, mint sms-t küldeni... Hát, majd ők egyszer felébrednek.

Amikor tényleg baj van...

Térjünk ki egy kicsit a baj esetén való eljárás kiveszésre, mert a szabályzatban ez is benne foglaltatik, ugyanakkor szeretném, ha tudnád, hogy mi ennek az alapelve, hogy könnyebben be tudd tartani, tartatni!

Az alapelv az, hogy kontárokra nem engedünk az adatok közelébe.

Kérdezd meg a Kürt Zrt. vezetőjét, Kürti Sándort, hogy a végleges adatvesztést mi okozza az esetek 80%-ában!

Azt fogja válaszolni, hogy a „kontár szakbarbárok”.

Az adat visszaállításra specializálódott cégek még a tűz emésztette merevlemezekről is nagy biztonsággal (79%) vissza tudják állítani az adatokat, de ha egy hozzáértőnek látszó amatőr (már elnézést) belekontárkodik, akkor az adatoknak végleg kampec.

Katasztrófa esetén a legfontosabb a merevlemez védelme, ennek első lépése az, hogy senkit nem engedsz hozzányúlni. Sem ismerőst, sem rokont, sem hozzáértő szomszédot, hanem csak olyan valakit, aki például szerződésben áll veled (akár szóbeli szerződésben), és vállalja a felelősséget.

Ezért aztán mindennél fontosabb, hogy most, amíg még semmi problémád nincs, **addig találj egy megbízható szakembert** - nem kell kimondottan informatikusnak lennie, elég, ha a közelben találsz egy szervizt, akiket többször is letesztelsz, hogyan bánnak az ügyfeleikkel :) -, és

megbeszéled vele, hogy gond esetén őt fogod hívni. És tényleg őt hívod.

Nem nyúlkálsz, nem kontárkods, nem zsonglőrködsz.

Míg a szakember kiérkezik, a géphez nem szabad nyúlni. Az a teendő ilyenkor, hogy szépen felvázolod akár egy darab papírra, hogy milyen sorrendben, milyen események követték egymást, mi volt az első, problémára utaló jel, mi volt a következő, stb.

Bár saját tapasztalatom az, hogy probléma esetén a felhasználóknak egy szavát sem lehet elhinni - úgy kell közelíteni a géphez, mintha ott találtuk volna, és ki kell deríteni mi a baja, mert a felhasználók szinte mindig másként értelmeznek dolgokat - de adatvédelmi szempontból ez így nem állja meg a helyét.

Adatvédelmi szempontból mindenképp az adatok mentésére, védelmére kell helyezni a hangsúlyt, de ezt a szakemberednek is tudnia kell. Mivel úgylis az adatok biztonságba helyezésével fog elsődlegesen foglalkozni, nyugodtan felvázolhatod neki az eseményeket, tüneteket, ez nem fogja tévútra vinni.

A fenti szabályzat néhány pontja magában foglalja az Adatvédelmi törvénynek megfelelő szabályokat. Erre nem térek ki külön, mert az egy külön tréning és 35 oldalas e-book témája lehetne (ráadásul nem velem, mert nem vagyok jogász), az adatmentésnek viszont csak egy részét képezi.

Házi Feladat!

Nyugodtan nyomtasd ki ezt az anyagot, és tanulmányozd át, add oda a családnak, és mondd meg nekik, hogy „ez a hibbant nőszemély” (ez lennék én:)) szabályok bevezetésére akar rábeszélni. *Érted? SZABÁLYOK!*

Igen, én is nagy szabadságharcos vagyok, és néha még anarchista is bizonyos tekintetben, de amit muszáj, azt muszáj.

Az általam felvázolt mintaszabályzat alapján skiccelj össze egy családon belüli szabályzatot, írd fel rá, hogy

- Mire és hogyan, milyen lépéseken keresztül történik az adatmentés.
- Ki, milyen adatokat ment.
- Mikor történik az adatmentés.
- Titkosítás esetét kifejteni.
- Katasztrófa közeli állapot esetén kit kell értesíteni és mit kell addig csinálni.

Ugye, hogy így már nem is olyan bonyolult? :)

Zárszóként

Már Te is láthatod, miért nem kaptál ilyen anyagot eddig soha. Eddig senkinek sem volt eddig kedve megmondani a felhasználónak, hogy: „Ide figyelj, butaságokat csinálsz. Azért, mert valamit LEHET, az nem azt jelenti, hogy SZABAD!”

Ezt nevezem én hasznos információnak, ezt egy újságcikktől vagy „anyázós” blogok bejegyzéseiből sosem fogod megkapni.

Most pedig, kérlek menj a blogra, és még most melegében írd meg a véleményedet a [Véleményem az Adatvédelmi és Adatmentési „Bibliáról”](#) című blogbejegyzés hozzászólásai közé.

[>>Kattints ide, és írd meg a véleményedet a támpontok alapján<<](#)

Köszönöm, hogy elolvastad, köszönöm, hogy használod, és köszönöm a véleményedet előre is!

Vidi Rita
www.viruskommando.hu