

BIZTONSÁGOS ADATKEZELÉS A MEREVLEMEZEN

Második, bővített kiadás – Global Union Kft., 2010. 05. 28.

Mint ahogy arra néhány, nemrégiben napvilágot látott cikk¹ rámutatott, a fénymásológépek és nyomtatók, amennyiben rendelkeznek merevlemezzel, azon sok bizalmas adatot tárolnak a szokványos munkamenetek során, és ezek törlése távolról sem teljeskörű. Ebben a leírásban részletesen bemutatom, hogy mit és hogyan tárolnak ezek a készülékek, illetve azok törlése hogyan történik, és mit tehetünk a legmagasabb szintű adatbiztonság eléréséhez.

Az adatok átmeneti tárolása

Minden, a multifunkciós készülékeken vagy nyomtatókon elkészített dokumentumot átmenetileg tárolja az adott készülék, amíg az adott munkamenet tart. Az így tárolt adatokat képként (bitmap, tömörítetlen képponthalmaz) kezeli a készülék, mert a nyomtatáshoz vagy a beolvasott fájl elkészítéséhez neki ilyen formában van rájuk szüksége. Ezeket az átmenetileg tárolt képeket az eszközök az adott munkamenet² végén törlik.

Erre miért van szükség?

Az analóg fénymásológépek idejében, ha több példányt kértem, azok annyiszor olvasták be az eredetit, ahány másolatot kellett készíteniük. Hatalmas előrelépés volt, amikor a digitális korszak kezdetével a másolást, mint tevékenységet felbontottuk szkennelésre és nyomtatásra. Az egyszer beolvasott képet annyi példányban tudjuk kinyomtatni a memóriából, amennyiben csak akarjuk (scan once, print many). Mivel ez a technológiai váltás a 90-es évek végén zajlott, még nem állt akkora terjedelmű olcsó RAM memória a gyártók rendelkezésére, mint manapság. Viszonylag rövid idő alatt kiderült, hogy a készülékek véges memóriakapacitása kevés, főként a nagy teljesítményű modellek esetében, ahol akár 100-200 lapos adagokban is másolnak a felhasználók. Egyetlen megoldás jöhetett csak szóba: a merevlemez. Ezek viszonylag olcsók voltak, és már az akkori kapacitásuk is több volt, mint elég, legalábbis erre a szintű felhasználásra.

Az adatok törlése a munkamenet végén

Amennyiben a szóban forgó készülék nem rendelkezik merevlemezzel, az átmenetileg tárolt képeket csak RAM memóriában tárolja, ami a folyamat végén onnan teljes törlésre kerül. A RAM memória másik tulajdonsága, hogy az adatokat csak addig tárolja, amíg áram alatt van – tehát ha kikapcsolom a főkapcsolóval a gépet, a RAM-ok teljes tartalma végérvényesen és visszavonhatatlanul törlődik.

Merevlemez esetében már más a helyzet. Ezek azon túlmenően, hogy áramtalanítás során sem veszítik el tartalmukat, lényegesen nagyobb tárhelykapacitással, de jóval alacsonyabb írási/olvasási sebességgel rendelkeznek, a RAM memóriákhoz viszonyítva. Ebből eredően már a korai PC korszaktól, ahol először megjelentek, úgy lettek kialakítva ezek az eszközök, hogy a lehető legjobb sebességet tudják produkálni. Amikor a merevlemez ír, akkor általában oda ír, ahol éppen tartózkodik a fej, és az adott szektor(ok) felülírhatók. A törlés úgy történik, hogy az őt vezérlő rendszer (PC, vagy a jelen esetben egy nyomtató/MFP) utasítja, hogy az adott fájl törölhető. A merevlemez törli az adott fájlra mutató bejegyzést a fájlok pozícióit tartalmazó táblázatából³, ezzel jelezve, hogy azok a szektorok, ahol ez a fájl található, a legközelebbi alkalommal már felülírhatók. Ez lehet percekben belül, de akár hosszú hónapok múlva is – előre nem jósolható meg.

Az adott munkamenet végeztével tehát a szóban forgó készülék, a munkamenet során ideiglenesen tárolt képeket nem törli le, csak bejelöli őket felülírhatónak. Egy kellő ismeretekkel rendelkező szakember az így "törölt" adatokat, az eltelt idő függvényében, akár teljes egészükben is vissza tudja állítani. Tekintettel arra, hogy a tárolt adat egy nyers képfájl, annak részleges felülírása sem jelenti a kép integritásának megbontásával a teljes kép használhatatlanná tételét – vagyis a megmaradt részlet még mindig megtekinthető marad, csak hiányozni fog egy rész belőle.

Az átmeneti képek biztonságos tárolása és eltávolításuk

A fent kifejtett probléma biztonságos kezelésére egy összetett eljárást fejlesztettek ki a mérnökök. Ennek egyik

1 CBS News (angol nyelvű) <http://www.cbsnews.com/stories/2010/04/19/eveningnews/main6412439.shtml>
IT café http://itcafe.hu/hir/fenymasolo_hdd_ftc_usa.html

index.hu - http://index.hu/tech/2010/05/19/a_fenymasolok_mindent_tarolnak/

2 Ha mindössze egy oldalt másolok, az egy munkamenet. Ha egyszerre beteszek 100 lapot a dokumentumadagolóba, az szintén egy munkamenet. Egy nyomtatás szintén egy munkamenet. Egy ilyen folyamat tehát a nyomtatás vagy szkennelés elindításától annak befejezéséig tart.

3 TOC – Table of Contents

összetevője az összes, merevlemezen átmenetileg vagy hosszabb távon⁴ tárolt adat titkosítása – tehát még ha vissza is tudja nyerni azokat egy szakember, a titkosító kulcs hiányában nem fogja tudni kikódolni azokat, és a másolt/nyomtatott/szkennelt képek helyett csak összevissza képpontokat fog látni. A titkosító kulcs egyedi, és a felhasználó tudja beállítani az első alkalommal, amikor a későbbiekben említendő adatvédelmi opciót telepíti a készülékén. Ezt a funkciót csak bizonyos, fejlettebb firmware-rel rendelkező típusok támogatják – további részleteket a lejjebb található táblázatban olvashat.

A védelem második lépcsője az adott munkamenet végén, az ideiglenes kép teljes, többszöri felülírása⁵. Ez hivatott pótolni a korábban említett hiányosságot, és bármennyire tűnik kielégítőnek az átmeneti adatok eltüntetésére alkalmazott módszer, de még így sem jelenthet 100%-os védelmet, csakis a titkosítással kiegészítve⁶. Természetesen a többszöri felülírás időt vesz igénybe, ezért ilyenkor a készülék, az adott munkamenet befejeztével még egy bizonyos ideig a törléssel fog foglalkozni, és csak ezután engedi majd új munkamenet indítását. Ez a biztonság ára – egy kicsit várni kell majd. A teljes törlés ideje az adott munkamenet során letárolt ideiglenes adatok méretétől függ majd.

Ez a két eljárás együtt már ellehetetleníti az ideiglenesen tárolt adatok részletekben vagy egészben történő visszanyerését bárki számára. Az itt leírt módszereket a Kyocera gépeken a Data Security Kit (adatbiztonsági készlet) nevű opció végzi. Az említett opció eleget tesz az ISO/IEC 15408-as szabvány⁷ által támasztott követelményeknek.

Az érintett Kyocera multifunkciós készülékek listája

TÍPUS	MEREVLEMEZ	SZÜKSÉGES OPCIO	TERMÉK STÁTUSZ	TITKOSÍTÁS
KM-6230	alaptartozék	nem elérhető	kifutott	nincs
KM-6330/7530	alaptartozék	nem elérhető	kifutott	nincs
KM-4530/5530	alaptartozék	nem elérhető	kifutott	nincs
KM-C830/850	opcionális	nem elérhető	kifutott	nincs
KM-C2630	opcionális	nem elérhető	kifutott	nincs
KM-3035/4035/5035	opcionális	Data Security Kit (A)	kifutott	nincs
KM-6030/8030	alaptartozék	Data Security Kit (B)	kifutott	nincs
KM-3050/4050/5050	alaptartozék	Data Security Kit (C)	kifutott	van
KM-2560/3060	alaptartozék	Data Security Kit (C)	kifutott	van
KM-C2520/3225/3232	alaptartozék	Data Security Kit (D)	kifutott	nincs
KM-C2525E/3232E/4035E	alaptartozék	Data Security Kit (D)	kifutott	nincs
TASKalfa 250ci/300ci/400ci/500ci/552ci	alaptartozék	Data Security Kit (E)	futó	van
TASKalfa 620/820	alaptartozék	Data Security Kit (B)	futó	nincs
TASKalfa 300i	alaptartozék	Data Security Kit (E)	futó	van
TASKalfa 420i/520i	alaptartozék	Data Security Kit (E)	futó	van

Az opció utólagos telepítése

Amennyiben enélkül a biztonsági rendszer nélkül használta a készülékét, és most fontosnak tartja a korábbi ideiglenes képek eltávolítását, valamint ezek biztonságos kezelését a jövőben, nincs egyéb dolga, mint telepíteni a készülékéhez tartozó adatbiztonsági készletet. Az első aktiváláskor – amennyiben a készüléke támogatja a titkosítást – kell majd megadnia a saját, egyedi titkosító kulcsát⁸, és ezt követően a készülék a merevlemezéről mindent el fog távolítani.

Innentől kezdve folyamatosan működik a biztonsági rendszer, és minden munkamenet végén a készülék kijelzőjén egy kis villogó ikon jelzi majd, amíg a merevlemezen ideiglenesen tárolt adatok teljes törlése zajlik. Csak ezt követően tudja majd folytatni a munkát.

⁴ Pl. a dokumentumfiókban lévő adatok, vagy a tárolt nyomtatások.

⁵ Ez három menetben történik meg. Az első két ciklusban az érintett szektorokat véletlenszerű adatokkal írja tele a készülék, a harmadik ciklusban pedig nullákkal (0x00).

⁶ Ebben az esetben ugyanis a nem ideiglenes adatok még később visszanyerhetők maradnak. Szerencsére azok a típusaink, amelyek sok adatot tárolnak így a merevlemezen, mind támogatják a titkosítást is.

⁷ Wikipedia - http://en.wikipedia.org/wiki/Common_Criteria

⁸ Ezt célszerű felírni, és egy lezárt borítékban elhelyezni egy biztonságos helyen (pl. páncélszekrény). Ennek hiányában ugyanis később még elveszíthet fontos adatokat, ha a készülékében panelt kell cserélni, és nem tudjuk újra megadni a korábban használt kulcsot.