

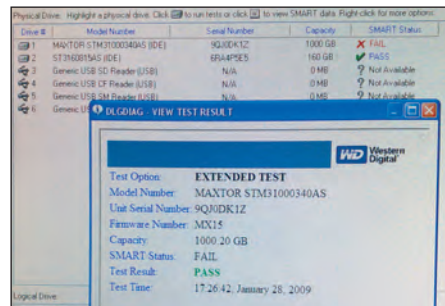
Zničte data!

Problematika ničení dat je velmi široká a dobře propracovaná. Přesto se stále objevují nové a nové případy rekonstrukce dat z vyražených nebo ztracených počítačů. Ničení dat se týká všech médií, papírových, magnetických, CD, DVD apod. K tomu jsou zpracovány postupy a normy, dokonce i podle požadované kvality a profesionality mazání (ničení) dat. Neří tedy třeba vymýšlet nic nového, ale ani tuhle oblast nepodceňovat. Doporučujeme začít na webových stránkách, třeba na rozcestníku [2], a poté si vybrat normu odpovídající potřebám uživatele.

Klíčové problémy ničení dat

Na příkladu si ukážeme, jaké problémy budeme řešit, jestliže bychom třeba prodáváli nebo dávali opravit notebook nebo PC. Především nevíme, co všechno operační systém někde zaznamenává a co všechno v počítači zůstalo. Viditelným, i když nikoliv nejnebezpečnějším příkladem mohou být soubory pagefile.sys a hiberfil.sys. Může v nich být i heslo, které jsme před chvílí zadávali k našemu internetovému bankovníctví. Může tam být kus textu, který jsme psali v MS Wordu, apod. Ostatně tyto informace mohou být z naší předchozí činnosti kdekoli na disku. Operační systém si s informací, kterou vkládáme, čteme nebo přenášíme, dělá v počítači v podstatě, co chce a my nemáme žádnou kontrolu nad tím, co kam запиše a co si kam dočasně uloží. Forenzní kriminalisté a vědci využívají právě tyto stopy, které po uživateli v počítači (nebo v mobilním telefonu) zůstanou (přestože se je „uživatelé“ někdy snaží i zničit). Nevěřte tomu, že když použijete program na ničení souborů, který slibuje, že soubor dvacetkrát přepíše, že tím zničíte veškerá data, jež se k tomuto souboru vztahují! Je zde velká pravděpodobnost, že „hlavní porce dat“ bude smazána, ale nikoliv všechna a nikoliv garantovaně. Operační systémy po každém zanechávají tak silnou stopu, že se jim samy dokážou po určité době „zaplevelit“, a musí se použít tzv. čisticí programy k jejich odstranění. Je-li třeba určitou informaci chránit, nezbyvá než zjistit, které fyzické nosiče ji mohou nést, a chránit nebo ničít tento nosič. U PC je to především pevný disk. Zdá se, že ho stačí zformátovat a pak přepsat náhodnými daty. Avšak ve špičkových laboratořích, které jsou na tyto postupy zaměřeny, je možné zjistit předcházející informaci do jisté míry i po jejím přepsání. Je ale také možné se dostat k informacím v těch sektorech disku, které on sám označil za vadné v důsledku poruchy a na něž nedovolí nikomu

nic zapsat. Porucha mohla narušit několik bitů a ve zbytku sektoru(ů) mohlo zůstat mnoho kilobajtů důležité nesmazané informace. K té se bez laboratoře nelze do-



Obr. 1 Terabajtový disk přestal fungovat

stat. Forenzní vědci nebo hackeři to umějí. Jinými slovy, tak jako nemůžeme důvěřovat operačnímu systému, nemůžeme důvěřovat ani pevnému disku. Dále jsou zde paměti typu RAM (SRAM, DRAM aj.). Nedávno bylo ukázáno, že starý předpoklad, že paměť typu RAM se smaže odpojením od napájení, je mylný. Pokud vědci dostanou paměť včas a zchladí ji (třeba nejprve rychle sprejem, než se paměť vyjme a umístí do správně mrazivého laboratorního přípravku), mohou z ní vyčíst naposledy uložené informace i několik sekund až týdnů po vyjmutí z PC. Takto byly zrekonstruovány právě klíče k šifrovaným diskům apod. Možnosti čtení klesají rychle s časem, takže je to pro nás záchrana, nicméně už je nutné na tuto věc pamatovat, např. jestliže je počítač pod napájením v určitém tzv. spícím módu apod.

Mobilní telefon

Jak zacházet s mobilním telefonem, když se porouchá? Lze ochránit data, která jsou v něm, před zvidavým opravářem (hackeřem)? U mobilního telefonu není pevný disk, ale zato několik druhů pamětí a operační systém, který je využívá, také jak zrovna chce, stejně jako u PC. Pokud je tzv. smažeme (např. dáme smazat telefonní seznam), vážně pochybujeme, že by je operační systém přepisoval, prostě jen uvolní paměť, stejně jako u pevného disku. Na rozdíl od PC však žádný pevný disk vyjmout nemůžeme a nemůžeme vyjmout ani paměti typu Flash a RAM (nebo jiné typy), které ho nahrazují. Také nevíme nic o tom, zda v telefonu je nebo není vnitřní záložní minibaterie a jaké typy pamětí „drží“ a co v nich je nebo může být. Když vyjmeme z telefonu „velkou“ baterii, mohou „vyprchat“ informace z pamětí typu RAM, ale v pamětích typu Flash zůstávají. Z hlediska ničení jsou na tom tedy paměť typu Flash a pevný disk stejně. Operační systém sám žádné funkce skutečného ničení uvedené paměti nenabídne a speciální utility nejsou k dispozici

(u žádného známého telefonu). Takže zde nemáme dokonce ani to málo šancí na ochranu našich dat jako u PC. A dáme-li telefon do opravy nebo obecně z ruky, dáváme tím k dispozici i to, co nevíme.

Profesionální ničení

Je známo mnoho případů (a studie to stále potvrzují), kdy byly v bazarech nalezeny pevné disky s citlivými daty z pojišťovnictví, vysokých škol, vojenská data apod. Disky se jevíly „čisté“, ale data na nich byla objevena nebo zrekonstruována komerčními programy anebo hackersko-forenzními technikami. Ve všech případech šlo o profesionální selhání či o prosté lajdactví. Bezpečnost paměťových, papírových, elektronických, tedy všech médií, která obsahují důležitá data, musí být zajištěna od jejich vzniku až po jejich zánik. Zánikem se jistě nemyslí, že papír zmačkáme a hodíme do koše nebo že v PC podobně smažeme soubor. Také nestačí disk přeformátovat nebo koš s papírem vysypat do popelnice. Obojí vyjde nastejno: kdo hledá, najde. Nemusí sice najít všechno, ale i jeden správný papír nebo nějaký ten kilobajt správné informace stojí za to.

Za chyby se platí

Jednou můj kolega potřeboval rychle uložit větší množství dat. Prostřednictvím webových stránek si zakoupil nový 1 TB pevný disk a kurýrem ho měl za dvě hodiny na stole. V nastalé nervózní situaci zapomněl (nebo nechtěl?) disk zavést jako plně šifrovaný. Při použití profesionálních programů pro šifrování celého disku (výborný je freeware Truecrypt) je totiž (velice správně!) celý disk při instalaci vyplněn náhodnými daty a zašifrován, což by při dané kapacitě přece jen určitou dobu trvalo. Po čase však disk přestal komunikovat (obr. 1). Co měl dělat? Odnést do prodejny a reklamovat? Co když ho ale technik zprovozní? Co když ho přijmou jako reklamaci a zprovozní ho potom? Použit ho nelze, vrátit také ne, což tedy do něj párkrát bouchnout kladivem nebo ho ponořit do vody, zastrčit do odpadků a zahrabat do popelnice? Jakákoliv z těchto možností je špatná; jediným správným východiskem bylo svěřit mi disk do péče. Z disku jsem vyjmul tzv. plotny, neboli skutečné nosiče informace, a podrobil je demagnetizaci žářem v krbu. Uvedený postup nebyl stoprocentně podle normy NSA, protože jsem nemohl zaručit, že nějaký ten milimetr kovu při hoření neodlétl třeba do popelníku krbu (a tam mohla určitá informace přečkat), ani jsem nezajistil, že z disku zbyl pouze rozdrčený popel. (dokončení v příštím čísle)

Vlastimil Klíma, nezávislý kryptolog