Nepropadejte zoufalství

V současném světě se stále častěji ukazuje, že jedním z faktorů, které rozhodují o úspěchu či neúspěchu, jsou informace. Správné informace ve správný čas a na správném místě. Někdy však může dojít k tomu, že důležitá data – a je jedno, zda firemní či soukromá – jsou najednou z různých příčin nedostupná nebo jim hrozí zničení. V případě hardwarové nebo softwarové závady či mechanického poškození nastupují specialisté na záchranu dat. A uživatele obvykle překvapí, co vše se dá zachránit...

Co vlastně je ztráta dat?

Z pohledu uživatele jde vždy o situaci, kdy nemůže pracovat s daty, která byla uložena na některém médiu používaném v oboru informačních technologií. Podle toho, zda je poškozené médium nebo data na něm uložená, se rozdělují příčiny ztráty dat na hardwarové a softwarové.

Hardwarové závady

K závadám hardwarovým dochází často v důsledku prostého mechanického opotřebení, přehřátí, atmosférického přepětí, požáru, povodně nebo selhání jiných částí zařízení, zejména zdroje. Na závadě pevného disku se velice často podílí ničím nepodložené přesvědčení uživatele, že disk je hermeticky uzavřen a tím pádem se do něj nemohou dostat žádné nečistoty. Opak je pravdou, filtrační vložka zachycuje jen malé množství nečistot a i takové kouření u počítače dokáže vytvořit „dehtové pohoří“, do něhož prostě jednou narazí hlavička, začne se obalovat nečistotami a velice brzy odfrézuje povrch disku. Dalším z faktorů, které výrazně ovlivňují dění v oblasti záchrany dat, jsou velmi časté záplavy. S pevným diskem, do něhož vnikne vlhkost nebo bahno, je třeba pracovat co nejdříve, neboť znečištěná voda je velmi agresivní a ve velmi krátké době poleptá kovové části disku i elektroniky tak, že záchrana v podstatě není možná.

K poškození média také dochází díky nevhodnému zásahu obsluhy – prudký pohyb s pracujícím diskem, vyjmutí média v době zápisu, nesprávné zapojení či zasunutí zařízení nebo úmyslné mechanické poškození (zaměstnanec chce zakrýt svou neetickou nebo trestnou činnost). Extrémním příkladem je vykradení objektu nevzdělaným zlodějem, který se obává poplašného zařízení a krumpáčem znehodnotí vše, co svítí a bliká...

Hardwarovou závadu lze typicky poznat podle zvuku, zařízení se chová jinak než obvykle, nevydává žádný zvuk nebo je naopak velmi hlučné, je cítit „elektrický“ zápach či jsou patrné změny v důsledku přehřátí (například u karet prohnutí nebo změna barvy). Rozhodně se nevyplácí zkoušet opakované starty v dobré víře, že se systém vzpamatuje. Pro pevný disk je vypnutí a zapnutí, tedy přistání a start, stejně kritické jako pro letadlo. Představte si, že jste na palubě onoho letadla a zálohujte, další start už se nemusí podařit vůbec...

Softwarové závady

Softwarové závady jsou ještě pestřejší. Velmi často jde o chyby obsluhy – nechtěné smazání souboru, adresáře, uživatelského profilu, odstranění digitálních fotografií z paměťové karty, formátování nebo inicializace média. Vždy záleží na tom, jak je příslušná funkce implementována. K laickému posouzení rozsahu škody pomůže zdravý rozum a znalost doby, po kterou se například formátovalo – dnešní počítače jsou sice velmi rychlé, ale pevné disky mají tak obrovskou kapacitu, že skutečné přepsání uložených informací by trvalo několik hodin – pokud je tedy „hotovo“ za pár vteřin, šance na záchranu je obvykle velmi vysoká.

Obtížnější závadou než smazání souboru je poškození jeho obsahu nebo přepsání jinými daty. Rozdíl je často dán mírou znalosti, protože jediný dobře popsaný souborový systém může hostit teoreticky neomezený počet různých formátů souborů a dostatečně známé jsou jen rozšířené formáty.

Poškození souborů způsobují i viry, a to buď tím, že vloží sami sebe do souboru obsahujícího spustitelný kód, nebo je přímo jejich hlavní funkcí poškození souborů některých typů. Dobrou ochranou proti virům je nejen antivirus, ale i souborový systém, který uchovává předchozí verze souborů a umožňuje jejich obnovu, jako je například Novell NetWare. Tato pomůcka se osvědčí i ve chvíli, kdy nejde o činnost viru, ale o chybu programu, kterým uživatel soubor modifikuje – návrat k předchozí verzi je nejjednodušší a dostatečně účinné řešení problému.

Záchrana dat

Klasická záchrana dat začíná analýzou stavu média nebo souborového systému, která musí být provedena na specializovaném pracovišti. Protože při práci s médiem může dojít k jeho poškození nebo k rozšíření stávajícího poškození, je vždy pořizována pracovní binární kopie. Pro čtení fyzicky poškozených médií se používají i metody, jako jsou například cesty pro průnik k systémům čipových karet – udržování nízké nebo vysoké teploty, skokové ochlazení, programově řízený zdroj napájení atd. Častou metodou je modifikace elektroniky disku, výměna hlaviček disku nebo přenesení média do jiného korpusu. Pro všechny tyto práce je třeba mít rozsáhlé zkušenosti a špičkové mechanické, elektronické a optické vybavení. Pokud ale aktivní povrch disku není odfrézován do podoby jemného prášku, vypálené CD není rozlámáno na kousky nebo paměťová karta shořelá na troud, velmi často se binární kopie podaří.

Softwarová záchrana používá nejčastěji 2 techniky: doplnění či modifikace - oprava systémových informací, které originálnímu operačnímu systému chybí, aby byl přístup k datům obnoven; a vyhledání a přečtení datových souborů specializovanými nástroji, které nejsou součástí původního operačního systému. Vzhledem k velikosti současných médií není jiná cesta než použití vyvinutých nástrojů možná, snad pouze diskety a SIM karty mají ještě rozsah zvládnutelný za pomoci binárního editoru a bezbřehé trpělivosti.

Všeobecně rozšířenou pověrou je, že firmy zabývající se záchranou dat mají nástroje pro záchranu, o kterých zákazník neví, a opravu snadno provedou spuštěním zázračné utility. Pokud takové nástroje existují, autorovi se bohužel nikdy nedostaly do ruky.

Do softwarových záchran dat se uživatelé často pouštějí sami, snad proto, že opravné nástroje lze používat opakovaně, nebo že restart je tak snadný. Základní zásadou je nezapisovat nic na jakkoliv

poškozený disk, a to ani v rámci opravy. Takový zásah je téměř nevratný. Navíc pustit se do vlastního výzkumu bez bezpečnostní binární kopie je vyslovený hazard.

Forenzní činnost a audit

V dnešním světě přibývá situací, kdy je třeba prokázat, že data určitého typu na médiu byla nebo nebyla uložena, že měla nebo neměla hledaný rozsah nebo že určitá operace byla nebo nebyla provedena. Podobné otázky lze zodpovědět i u těžce softwarově i hardwarově poškozených médií. Nejčastěji je podobná zakázka zadána policejním vyšetřovatelem a to obvykle nikoliv jen u případů počítačové kriminality, ale například při podezření z odstranění účetnictví nebo skladové evidence. Soukromé subjekty se spíše zaměřují na preventivní opatření a zadávají forenzní audit svých systémů s cílem odhalit a odstranit potenciální možnosti úniku důvěrných informací. Audit musí být velmi komplexní a zaměřený dovnitř firmy nebo instituce, neboť více než 60 % úniků mají na svědomí vlastní zaměstnanci a cenné informace lze koupit i v podobě odpadkového koše ze správné kanceláře.

Představa, že počítačovou kriminalitu páchají zejména mladí hackeři ze svých temných doupat, je sice romantická, ale nikoli pravdivá. Obor záchrany dat se může snadno nevědomky stát nástrojem takové činnosti, když si zakázku zadá osoba, která se například neautorizovaně dostala k vyřazenému počítači, jehož disk nebyl dostatečně vymazán.

Odstranění dat

Odstranění dat je činností zcela opačnou než záchrana a jejím cílem bývá zamezit neautorizovanému přístupu k datům, která byla na médiu uložena. Bez smazání dat například nelze vyřadit a „vyhodit“ disk použitý v některé instituci která pracuje s utajovanými skutečnostmi. V poslední době tuto službu stále častěji vyhledávají i soukromé subjekty obávající se průmyslové špionáže. Odstranění dat není tak snadné, jak by se po popisu všech možností ztráty dat mohlo zdát. Existují metody, které dovedou bezpečně přečíst původní data na pevném disku i z místa, které bylo následně třikrát přepsáno. Podstatou je analogové ovzorkování povrchu disku a následná analýza na superpočítači Cray.

Není to nic mimořádného...

Ztráta dat je stejně běžná jako úrazy. Pokud se něco takového přihodí, je třeba neváhat a obrátit se na specialisty.

A na závěr jedna ekonomická zajímavost: Objem provedených záchran velmi dobře vypovídá o úrovni rozvinutí IT technologií v dané zemi. Česká republika má přibližně stejný objem záchran jako Polsko, ale více než čtyřikrát méně obyvatel.

Autor je ředitelem TDP-Ontrack Data Recovery, s. r. o.