

Metody záchrany dat při forenzním auditu

Záchrana dat jako služba má velmi široký záběr z mnoha úhlů pohledu. Předmětem záchrany může být (a v poslední době rozhodně je) jakýkoli nosič dat od velkých diskových polí přes disky a flash paměti až po vypalovací média. Formát, organizace a kontext dat na nosičích se liší podle použitého souborového a operačního systému a pokud postoupíme o stupínek výše, tak i podle aplikace, která pro uložení svých dat služeb souborového a operačního systému využila.

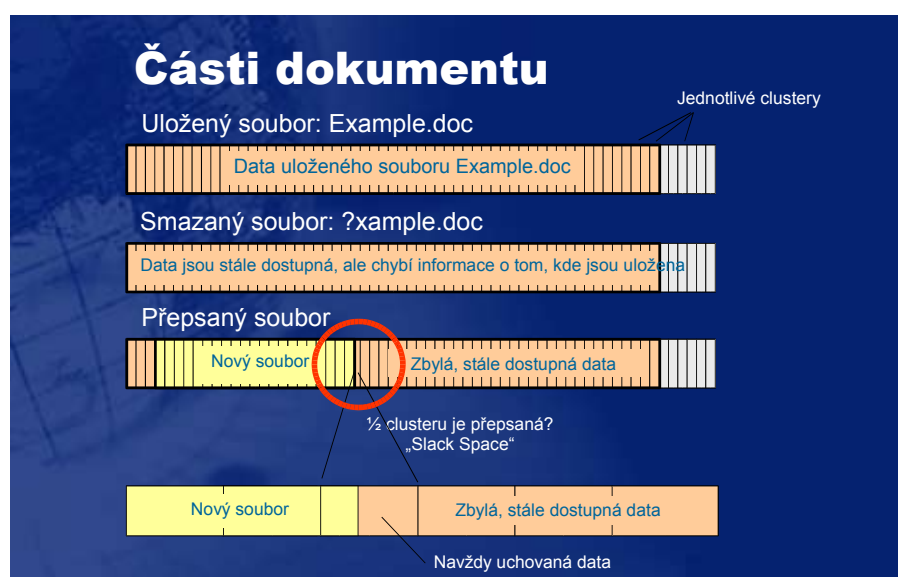
Základním předpokladem pro úspěšnou záchranu dat je hluboká interní znalost techniky zařízení/nosiče, souborového systému, operačního systému a aplikace, a to nikoliv z pohledu aplikačního programátora nebo technika, ale spíše z pohledu konstruktéra nebo tvůrce-vývojáře. Záchrana dat je používána vždy, když některá informace chybí (oblast SW problémů) nebo je nečitelná (oblast HW problémů). Interní znalosti jsou pak nutné k tomu, abychom mohli zařízení alespoň v laboratorních podmínkách zprovoznit nebo chybějící informace odvodit či vhodně nahradit a dosáhnout tak cíle – obnovení maximálního možného množství dat.

V reálném světě ovšem ke ztrátám dat nedochází jen z důvodu zásahu vyšší moci, opotřebení či neúmyslného omylu. Forenzní audit se zaměřuje na odhalení nebo prokázání účetních podvodů, zpronevěř a obdobných protiprávních stavů a jednání, což se v dnešní době téměř výhradně děje za plné nebo alespoň částečné podpory počíta-

čů. Navíc se může jednat i přímo o zneužití (vynesení, znehodnocení) počítačových dat, které nemá přímou nebo žádnou souvislost s účetní, skladovou, logistickou apod. operací.

Osoba, která se takového jednání dopouští, si je velmi často vědoma toho, že použitím počítače zanechává stopy a proto se snaží je zahladit. Zejména v situacích, kdy na počítači dojde přímo k provedení operace nebo operací, méně v situaci, kdy je počítač použit ke komunikaci (elektronická pošta, dokument, tabulka, vyplnění

formuláře na web serveru apod). Způsob, který uživatel zvolí pro zahlazení stop odpovídá míře znalostí výpočetní techniky a zabírá podle zkušeností, které jsme získali za mnoho let práce, vše, od smazání a vyčištění dat přes rozbití disku sekerou až po úmyslné založení požáru. Úplná likvidace dat, která by zároveň neodhalila hned původce, je ale velmi obtížná a bez speciálního vybavení v podstatě nemožná. Při použití běžných programových prostředků může dojít k situaci jako na obr. 1.



obrázek 1

Vzhledem ke způsobu dělení prostoru na bloky (clusters) nemusí vždy dojít ke spolehlivému přepsání všech informací. Scan disku který „rozumí“ formátům používaným aplikacemi jako jsou textové a tabulkové procesory naznačený zbytek nalezne a extrahuje. Bloky mají podle kapacity zařízení až desítky kB a lze takto nalézt i třeba celou jednu verzi dopisu, emailu nebo dat, která byla při procesu tisku uložena ve vyrovnávací frontě.



obrázek 2

Při záchraně dat je vždy cílem obnovit obsah, formát i kontext dat v maximální možné míře. Při forezním auditu ale často postačí prokázat nebo nalézt pouze kontext, kontext a fragmenty obsahu nebo pouze fragmenty obsahu. Podobá se to policejní práci, kdy podezřelý může jen obtížně tvrdit, že oběť neznal, když má ve svém mobilu uloženo její číslo a v kalendáři záznam o schůzce. Obdobně při počítačovém forezním auditu hledáme, zda se na počítači nebo jiném zařízení pro zpracování dat vyskytl nějaký dokument, byla nějaká data vytištěna, exportována, odeslána nebo přijata a to například s ohledem na výskyt textu, který charakterizuje prošetřované podezření.

Při komplexním auditu je postup obecnější a metody záchrany dat

jsou jednou z několika cest jak data shromáždit, protože jak je naznačeno na obr. 2, pracuje se i s daty, která nijak skryta nebo poškozena nejsou, analyzují se a skenují papírové dokumenty, zálohy, archivy atd. Shromážděná data jsou vyčištěna a indexována, což umožňuje jejich důkladné zkoumání a nalezení skutečně všeho, co se týká třeba konkrétního obchodního případu. Tyto služby jsou poskytovány auditorským firmám, kriminalistům i vlastníkům dat. Metodu ale lze s výhodou uplatnit i tehdy, kdy k žádnému zločinu nedošlo - například při fúzi firem HP a Compaq byla tímto způsobem sjednocena dokumentace zejména v oblasti obchodních, marketingových a právních dokumentů. Různorodost dat by ani jiný způsob reálně neumožnila. Například

firma Novell Inc. při konsolidaci informačních systémů zjistila, že důležitá data se vyskytují ve 160 (!) různých systémech od textových procesorů a tabulek až po personální systém a účetnictví.

Technické možnosti laboratoře pro záchranu dat jsou v některých ohledech stejně šokující jako schopnosti lékařské vědy. Sama možnost nalezení nebo prokázání dat naznačeným způsobem ale nedává záruku, že výsledky auditu budou správné a objektivní. Proto je technická a zejména právní konzultace na prvním a nikoliv posledním místě.

Václav Šamša

Autor pracuje ve společnosti TDP-Ontrack