Zničte data!

(dokončení z minulého čísla)

V minulém čísle jsme poukázali na to, že kromě dokonalého fyzického zničení paměťového média neexistuje žádný jiný způsob, který by laikovi zaručil, že na něm nezůstaly informace, které chce zničit. Problematika ničení dat je velmi široká a dobře propracovaná. Přesto se stále objevují nové a nové případy rekonstrukce dat z vyřazených nebo ztracených počítačů. Ničení dat se týká všech médií, papírových, magnetických, CD, DVD apod. a jsou k tomu zpracovány postupy a normy, dokonce i podle požadované kvality a profesionality mazání (ničení) dat. Není třeba vymýšlet nic nového, ale ani tuhle oblast nepodceňovat, jak již bylo řečeno. Doporučujeme začít na internetu, třeba na rozcestníku [2], a poté si vybrat normu odpovídající potřebám uživatele.

Pevné disky

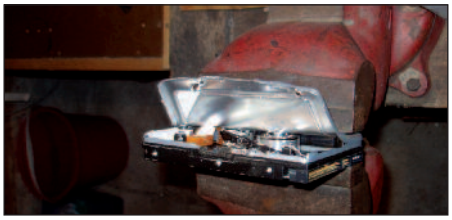
V případě pevných disků nelze spoléhat ani na profesionální programy na mazání dat, i kdyby je přemazávaly stokrát. Na pevném disku může být oblast, která je označena za vadnou, a tam se žádný program nedostane. Je možné tomuto argumentu oponovat? Jako řešení se jeví nejprve disk celý zašifrovat, neboli docílit toho, že na disk se od samého počátku nikdy nic jiného než šifrovaná data nedostane. Pak by nám nevadil ani později vzniklý vadný sektor! Profesionálové v oblasti ochrany dat (chcete-li, dosaďte si termín paranoici) by namítli, že to je pravda, ale co když bude šifrovací klíč kompromitován? V takovém případě se šifrovací klíč vymění a potenciálně ohrožená data se přešifrují jiným klíčem. Ovšem pozor, zašifrovaná data ve vadných sektorech jsou chráněna kompromitovaným klíčem, tedy jako by nebyla šifrována. A jsme tam, kde jsme byli na začátku. Argument z jiného soudku je ten, že činností operačního systému napadeného malwarem nebo chybou pevného disku nebo jakoukoliv jinou potenciální softwarovou či hardwarovou chybou, úmyslnou nebo neúmyslnou, se může dostat otevřená informace na pevný disk. Žádný výrobce operačních systémů, programů nebo pevných disků nikdy nezaručí, že se to nestane. Profesionál je tedy kupodivu ve stejné situaci jako laik – aby měl stoprocentní jistotu, musí paměťové médium dokonale fyzicky zničit. Rozdíl mezi nimi je jen v tom, že profesionál ví proč, zatímco laik si myslí, že je paranoik.

DVD, CD, RAM, flash

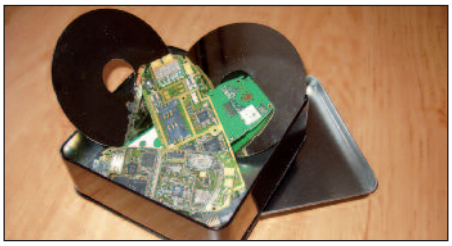
Podobné je to i s DVD, CD, paměťmi flash, a dokonce i paměťmi RAM (v předchozím čísle jsme se zmínili o možnosti číst informace z paměti RAM i po odpojení napájení). Jejich rozlomení nebo rána kladivem se rovná jejich zničení jen proti laickému zneužití.

Mobilní telefony

U mobilních telefonů je pro laika situace ještě složitější, protože z nich nemůže vyjmout



Obr. 2 Vyjmutí ploten pevného disku



Obr. 3 Příprava domácí pece do krbu

Obr. 4 Laicky fyzicky zničená data

pevný disk a netuší, jak vymazat paměť flash. Neví, zda v mobilu je nebo není miniaturní baterie, která drží obsah paměti, jaký typ paměti to je, kde je a co je v ní uloženo za informace. Jistěže i laik může mobilní telefon rozebrat. Co ale bude dělat s miniaturní baterií, která je tam přiletovaná, to netušíme.

Paranoici a paranoici

Na zavedení šifrovaného pevného disku je mnoho pohledů. Z hlediska běžného uživatele paranoidní opatření, z hlediska bezpečnostního profesionála ochrana dat na vyšším stupni. Z hlediska výrobce pevného disku, operačního systému nebo šifrovacího softwaru opatření, která vám doporučí, ale nikdo z nich nebude garantovat nic, co by vám pomohlo. Jediné, co je stoprocentní pro laika i odborníka, je paměťové médium (papírové, magnetické nebo jiné) rozmetat na atomy. Tím se zničí to, co informaci uchovávalo – jedinečné spojení atomů tohoto média. Tedy papír spálit a popel rozdrtit, disky roztavit (s teplotou zajišťující demagnetizaci) a rozdrtit na prach apod. To říkají profesionální normy! Spoustu norem na skartaci dat a seznamy schválených zařízení na ničení jednotlivých typů nosičů (HDD, DVD, papírů apod.) lze snadno nalézt na internetu. Rozlišují, i jaký stupeň ochrany má ničení zajistit, a podle toho jsou konstruována různě drahá ničicí zařízení (na bázi různě drahých technologií). Netřeba tedy nic vymýšlet, jenom si uvědomit rizika a podle toho se zařídit. Jistě víte o tom, že integrované obvody v mobilu (*obr. 3 a 4*) jsou schopny desítky vteřin přežít bez poruchy (!) několik set stupňů Celsia. Avšak pokud běžnému uživateli doslouží starý počítač, nemusí ho házet do vysoké pece (jako se ničí profesionální šifrátory) ani pálit pevný disk (*obr. 2*) v krbu. Minimálně asi použije program na mazání pevného disku (z článku vyplývá, že profesionální a freewarový program se liší v zásadě jen velmi málo). Potom může počítač dát do kontejneru s dosloužilou elektronikou nebo do bazaru. Článek měl jen upozornit na to, že zde i přesto existují určitá rizika. Jestliže je uživatel akceptuje v závislosti na ceně zbytkových dat, je to v pořádku, horší je o nich nevědět. Když někdo zodpovídá za ochranu dat v organizaci, vyplatí se počítat, jak dlouho bude mazat data softwarovými nebo hardwarovými prostředky na médiích nebo počítačích a jak velké riziko odhalení zbytkových informací tímto (velmi často negarantovaným) mazáním podstupuje. Možná zjistí, že se vyplatí si pořídit profesionální ničič datových médií, kde za mnohem kratší dobu garantovaně zničí větší množství médií, nebo se takto podaří zdůvodnit pořízení krbu do pracovny bezpečnostního ředitele. Bezpečnostní ředitelé se mohou opřít o to, že každá kancelář v NSA má svoji skartovací pícku. Možná je to předzvěst komerčních pícek. Dříve byly skartovačky na papír také jen v bezpečnostních složkách a v současné době je lze nalézt v každé bezpečnější kanceláři. Budou tam za deset let také skartovačky elektronické? Mimochodem, víte o tom, že v USA existuje národní společnost pro destrukci dat (NAID)?

Závěr

Závěrem lze říci, že šifrování datových médií je velmi dobré opatření na pokročilé úrovni ochrany dat, ale některá rizika zůstávají. Byly zde ukázány skryté hrozby i možnosti ničení dat na různé úrovni.

Vlastimil Klíma, nezávislý kryptolog,
v.klima@volny.cz

LITERATURA:

[1] Archiv autora a článků kryptologie pro praxi: http://cryptography.hyperlink.cz.

[2] http://en.wikipedia.org/ Data_erasure, Data_remanence.