Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství

Bakalářská práce

Bezpečnost mazání dat, zejména citlivých dat

Filip Honč

! ! !

Místo této strany vložíte zadání bakalářské práce.

(Do jedné vazby originál a do druhé kopii)

! ! !

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Bezpečné mazání dat, zejména citlivých dat" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 29.2.2012 _____

Poděkování

Rád bych touto cestou poděkoval RNDr. Dagmar Brechlerové, Ph.D. za odborné vedení a cenné připomínky při zpracovávání této práce.

Bezpečné mazání dat, zejména citlivých dat

Secure data erasure, particularly sensitive data

Souhrn

Tato práce je zaměřena na bezpečnost dat z hlediska jejich mazání z fyzických médií. V dnešní době je stále mnoho uživatelů počítačů přesvědčeno, že stačí pouze data odstranit z „koše“, což dokládají i výsledky dotazovaných respondentů. Práce je především zaměřena na dnes nejpoužívanější datová média, a těmi jsou pevné disky, založené na magnetickém zápise. Každý uživatel dnes musí počítat s tím, že jeho data jsou zneužitelná, a to buď k sociálnímu útoku, anebo přímo k vykrádání účtů. Proto je důležité věnovat se této problematice jak při odstraňování, tak při opětovnému prodeji datových médií.

Summary

This work is focused on data security in terms of their erasing from physical media. Today, many computer users still believe that you only remove data from the "basket", as evidenced by the results obtained from respondents of a survey. Primarily, the work is focused on the currently most common storage devices, i.e. hard drives that are based on magnetic record. Nowadays, each user must count with the fact that his/her data are exploitable, either for a social attack or directly to stealing accounts. Therefore it is important to pursue this issue, especially when removing or selling data media.

Klíčová slova:

Bezpečné mazání dat, osobní údaje, likvidace nosičů, obnova dat, magnetizace, šifrování dat, remanence, opakovaný přepis, přepisovací software.

Keywords:

Secure data erasure, personal data, disposal of data media, data recovery, magnetization, data encoding, remanence, repeated rewriting, rewriting software.

Obsah:

Seznam obrázků:

1 Úvod

Téma bakalářské práce bylo zvoleno z důvodu autorova dlouhodobého zájmu o datové nosiče a vše, co je s tím spojeno, tedy mazání i obnovu dat, likvidaci nosičů a v neposlední řadě i šifrování dat. Dalším důvodem jsou množící se aféry s úniky citlivých informací z velkých podniků, případně přímo ze státní správy.

Práce je rozvržena do dvou větších celků. V první části se autor věnuje bezpečnému mazání citlivých dat. Tato část v sobě zahrnuje techniky mazání, fyzickou likvidaci a nástroje, které s touto problematikou souvisí. K této části se autor rozhodl připojit i malý přehled legislativních opatření uplatňovaných v České Republice a jiných zemích. V druhé části autor pojednává o možnostech obnovy dat na různých typech datových nosičů, a to jak softwarovou cestou, tak i laboratorní analýzou. V této části se též okrajově zabývá technikou, jak maximálně ztížit získání informací z uniklých dat, a to šifrováním.

Je až s podivem, kolik uživatelů počítačů si v 21. století neuvědomuje rizika spojená se ztrátou dat, která může vést až ke ztrátě finančních prostředků. Kromě přímé a vyčíslitelné ztráty můžou vzniknout i jiné újmy, od ztráty přístupů k nebankovním účtům až po odhalení nepříjemných, či dokonce kompromitujících materiálů.

Ve firemním sektoru se zdá být situace o mnoho lepší, ale může jít jen o klamný obraz, který velké společnosti vytvářejí. Na českém trhu operuje také velké množství menších firem, jejichž zabezpečení, například zákaznických dat, není zrovna ideální, a to i přesto, že za takovýto unik dat můžou hrozit nemalé postihy.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem práce je prozkoumat, zda, a pokud ano, tak do jaké míry, obyčejní uživatelé počítačů i zkušenější technici informačních systému znají metody odstraňování dat a dokážou rozpoznat rizika s nimi spojená. Autor se samozřejmě zaměřil na zneužitelná data.

Na základě několikaletých osobních zkušeností předpokládá, že povědomost široké veřejnosti o této problematice je krajně nedostatečná.

Práce by měla čtenáři poskytnout ucelený obraz o metodách nakládání s datovými médii a také poodhalit rizika spojená s nechtěným únikem citlivých dat.

2.2 Metodika

Metodika práce byla zvolena s ohledem na zpracování a vyhodnocení dat formou dotazníku (viz příloha 01) o 10 otázkách. Otázky byly formulovány s důrazem na objektivitu a smysluplnost. Některé otázky nabízely možnost volby doplňkové odpovědi.

Dotazník byl vytvořen na serveru http://oursurvey.biz a prostřednictví mnoha komunikačních kanálů rozeslán běžným uživatelům internetu, a k tomu speciálně zaslán i na IT oddělení vybraných podniků ve státní i soukromé sféře. V okamžiku ukončení dotazování se šetření zúčastnilo 197 respondentů. Vyplnění dotazníku trvalo účastníkům v průměru 2 minuty. Následně byly dotazníky vyhodnoceny a účastníci rozděleni do několika věkových a znalostních skupin. Odpovědi od IT pracovníků byly zahrnuty do samostatného vyhodnocení.

K doplnění dotazníku zvolil autor praktický test formou experimentu. Opatřil si dva použité pevné disky a pokusil se z nich získat nějaká „zajímavá“ data. První byl zakoupen na inzerát, jednalo se o SATA harddisk od výrobce Seagate, konkrétně 80GB Barracuda 7200.9 z roku 2006. Druhý harddisk získal z jedné záměrně nejmenované firmy z počítače určeného k likvidaci, respektive k odvozu v rámci systému REMA – ekologického nakládání s elektroodpadem. V tomto případě se jedná o starý, opotřebovaný IDE disk od výrobce Western Digital, konkrétně 40GB WD Caviar 400 z roku 2003. Data se podařilo vcelku snadno obnovit, více v samostatné kapitole 4.6.

Práce vychází ze vstupní hypotézy, že uživatelé i podniky podceňují možnosti úniku citlivých dat právě cestou získání použitého, či vyhozeného „smazaného“ datového nosiče a jeho následné kompletní nebo částečné obnovy.

3 Bezpečné mazání citlivých dat

3.1 Mazaní dat z hlediska nejpoužívanějších systému souborů.

Zpracováno podle [13]

Systémů souborů je nepřeberné množství, a proto se autor zaměřil hlavně na ty nejpoužívanější na pevných discích. Jako základní rozdělení zvolil rozdělení na systémy souborů požívané operačními systémy MS Windows a Unix-based OS.

3.1.1 Systémy souborů používané ve Windows

Operační systémy od Microsoftu používají zvláště dva systémy souborů. Jsou to už poměrně starý systém FAT, a o mnoho novější NTFS. Systém souborů FAT je dlouhodobě na pevných discích na ústupu – zvláště kvůli omezeným možnostem adresace dat, ale na přenosných flash discích je stále naprosto běžný.

3.1.1.1 Souborový systém FAT

Systém souborů FAT (File Allocation Table) byl představen v roce 1977 se zaměřením na disketové mechaniky, jeho úplně první verze byla pouze 8mi-bitová. Postupně se z ní stal hlavní diskový systém souborů. Následující hlavní verze jsou FAT12, FAT16 a FAT32. Poslední verze FAT32 byla představena v roce 1996 se systémem MS-DOS 7.1 s nadstavbou Windows 95, avšak nativní podpora byla až v systému Windows 2000. Na vývoji tohoto systému se postupně podílelo několik firem, a to Microsoft, SCP, IBM, Compaq, Digital Research a Novell. Limitujícími faktory poslední verze jsou zvláště maximální velkost souboru (zjednodušeně 4GB), maximální velikost jednotky (zjednodušeně 2TB) a omezení týkající se délky a použité znakové sady jmen souborů.

Každý soubor ve FAT souborovém systému má svůj záznam v alokační tabulce souborů, která se nachází v prvním sektoru každé logické části disku. Pro případ poškození této tabulky je tu obvykle minimálně jedna její kompletní kopie uložena bezprostředně za originálem. Alokační tabulka souborů obsahuje informace o tom, které clustery se vážou k tomu, či onomu souboru. Dále si udržuje informace o volných a vadných clusterech disku.

Další speciální tabulkou, nebo spíše jednoduchou databází, je tabulka adresářů, která obsahuje hlavně informace o jménu, jeho počátečním clusteru, celkové velikosti souboru anebo adresáře. Každý soubor je zde reprezentován záznamem o délce 32-byte (FAT32). Pokud operační systém hledá soubor, nalezne ho v adresářové struktuře kořenového adresáře, přistoupí k jeho prvnímu clusteru a s použitím alokační tabulky souborů zjistí, kde se nachází všechny jeho části.

Je proto velmi důležité si představit, že v případě smazání souboru dojde jen k jeho výmazu z adresářové struktury a alokační tabulky souborů, ale samotná data jsou stále na disku přítomna. Tento fakt je také důvodem, proč lze tato data znovu obnovit softwarovou cestou.

3.1.1.2 Souborový systém NTFS

Souborový systém NTFS (New Technology File System) byl představen v roce 1993. Inženýři Microsoftu na něm pracovali od poloviny 80. let při současném zahájení vývoje Windows NT. Nový systém byl navržen s vidinou toho, aby splňoval nejenom veškeré současné, ale i předpokládané budoucí požadavky, které se objeví s vývojem nového hardwaru. Celý systém je řešen jako obrovská databáze. První verze 1.0 byla poprvé nasazena na systému „Windows NT 3.1“. Zatím poslední verze kompletního NTFS systému je 3.1 uvedená společně s Windows XP z roku 2001.

Vzhledem k tomu, že se vývojáři FAT bezpečností souborového sytému příliš nezabývali, vývojáři NTFS včlenili do vznikajícího souborového systému nový bezpečnostní model. Tento systém souborů je označován jako žurnálový souborový systém, protože používá speciální NTSF Log ($LogFile), který zaznamenává metadata o všech změnách na logické jednotce. Oproti systému FAT, který nemá žádné opatření proti chybám na disku, je to obrovská výhoda, protože při havárii systému se struktury FAT mohou stát nekonzistentními, což může způsobit ztrátu dat, nebo v horším případě kolaps celého souborového systému. NTFS se díky zabudovanému transakčnímu zaznamenávání akcí může při pádu systému pokusit obnovit data při jejich minimální ztrátě a všechny rozpracované operace dokončit nebo zrušit, a tím pádem systém souborů opět uvést do konzistentního stavu.

Na rozdíl od FAT je tabulka souborů uložena v novém „formátu“ MFT (Master File Table). MFT (soubor $MFT) udržuje informace o všech souborech, adresářích a metadatech na disku a je stejně jako FAT uložena na začátku logického oddílu, ale její kopie ($MFTMIRR) je uložena zhruba uprostřed logického prostoru. Je třeba ještě dodat, že tato kopie obsahuje pouze prvních 16 záznamů původní tabulky. Kromě výčtu clusterů obsahující data konkrétního souboru je tu nové pole pro seznam atributů, které popisují uložená data anebo typ uložených souborů. Na rozdíl od FAT tabulky jsou samostatně vyčleněny metadatové soubory pro vadné clustery.

$Badclus, který drží seznam známých vadných clusterů, které znovu nebudou použity; pokud nastane chyba při čtení dat, systém označí clustery za špatné a $Badclus se aktualizuje

$Bitmap je jednorozměrné pole bitů, které slouží ke sledování volného místa; když je bit 0, je volný, v opačném případě je použitý

[7]

Další podstatnou změnou oproti FAT systému souborů je, že FAT používá pro jména souborů 8-bitové ASCII kódování. Oproti tomu je v NTFS nasazeno 16ti-bitové kódování Unicode, což zpřístupnilo pojmenování souborů v jakémkoliv jazyce. Neméně zajímavá potom zůstává i podpora komprese celého souborového systému pomocí algoritmu, označeného jako LZNT1 (varianta LZ77), a podpora šifrováni dat EFS (Encrypting File System) implementovaná do vybraných vyšších verzí operačního systému Windows Vista a Windows 7. Je nutno se také zmínit o podpoře hardlinků a softlinků – speciálních záznamů vedoucí k souborům umístěným v jiné složce, v případě softlinků to může být i v jiném systému souborů. Co se týče limitů velikosti logické jednotky a jednotlivých souborů, v současnosti zdaleka přesahuje běžné potřeby. V současné implementaci je velikost souborového systému 256 TB (terrabyte), 16 TB je určeno pro jednotlivé soubory.

Přestože je koncepce systému NTFS velmi odlišná, mazání dat je velmi podobné systému FAT. V případě smazání souboru dojde k tomu, že je v tabulce MFT označen jako smazaný (ale zůstává v ní zapsán) a jeho clustery jsou v metasouboru $Bitmap označeny jako prázdné. Už z tohoto konceptu je opět vidět snadná obnovitelnost těchto dat.

3.1.2 Systémy souborů používané v Unixových systémech

Systémy vycházející z Unixu používají souborové systémy, které vychází z původního souborového systému, který neměl žádné konkrétní jméno. Byl označován jen jako FS (file system). Jeho vylepšení, o které se postarali studenti univerzity z Kalifornské Berkley, se nazývá UFS (Unix file system). Tento systém se stal skutečným předchůdcem současných Unixových souborových systémů.

3.1.2.1 Souborový systém „ext“

Souborový systém ext (extended file system) byl představen v roce 1992. Jedná se o první souborový systém, který byl vyvíjen speciálně pro systémy založené na Linuxovém jádře. Vývojáři se nechali inspirovat souborovým systémem UFS. Za hlavního vývojáře je zpravidla označován Francouz Rémy Card. Ext byl první systém souborů pro Linux, který implementoval VFS (virtual file system), tedy abstraktní vrstvu nad fyzickým souborovým systémem. Jeho poslední verze ext4 je velmi blízká předchozí verzi ext3, která je stále velmi hojně používaná. Od verze ext3 přibyla podpora žurnálování, a to hned na několika možných úrovních. Od žurnálovaní kompletních dat (nejbezpečnější) až po žurnálování pouze metadat.

Finální verze ext4 byla představena v roce 2008 a vznikla postupně ze série kompatibilních rozšíření k ext3. Nejvíce z nich vyvinula firma Cluster File Systems původně pro Luster souborový systém. Byly zvýšeny limity systému na 16TB pro soubor a 1EB (exabyte=10^{18} bytů) pro celý svazek. Fyzický disk je rozdělen do bloků a bloky jsou soustředěny do větších skupin. V každé skupině bloků je uložena mapa bloků mapa i-uzlů (inodes), tabulku i-uzlů a samotné datové bloky.

I-uzel je datová struktura, ve které se uchovávají metadata o všech souborech a adresářích v unixových souborových systémech. V i-uzlech se uchovávají informace o typu souboru, odkazech na něj, tzv. hardlincích, vlastníku a přístupových právech. Dále odkazuje na příslušné datové bloky, velikost a časové značky.

Pokud uživatel zvolí smazat určitý soubor, tak se v příslušném i-uzlu sníží počet hardlinků o jeden. V případě, že soubor neodkazuje do nějaké jiné složky, bude počet

hardlinků roven nule a obsah i-uzlu se vynuluje. Vzhledem k tomu, že se vymažou informace vedoucí k určení polohy dat na disku, je softwarová obnova daleko složitější. Musí se zanalyzovat žurnálovací soubory, a ani tehdy není výsledek stoprocentně jistý. Proto se dá považovat ext4 systém souborů za mnohem bezpečnější z hlediska mazání dat než zatím vyjmenované.

3.1.2.2 Souborový systém HFS

Souborový systém HFS (Hierarchical File System) byl představen v roce 1985 firmou Apple Computer. První podpory se dočkal v systému „System 2.1“, konstruovaném na počítače Macintosh. Tento souborový systém vyšel jako náhrada pouze o rok staršího MFS (Macintosh File System), který byl však v mnoha ohledech nedostatečný. Od svého vzniku dodnes prošel jen několika významnými updaty a základní struktura původního, aktuálně 27 let starého, souborového systému je víceméně nezměněna. Vše vychází ze speciální stromové metadatové struktury, označené jako B-strom, která se snaží minimalizovat čas potřebný k vyhledání a nalezení cesty ke konkrétnímu souboru. Význam počátečního písmena názvu nebyl nikdy upřesněn, ale nejčastěji se má za to, že je odvozen od slova balanced (vyvážený).

Poslední a zároveň druhou hlavní verzí je HFS Plus, který byl vyvinut opět z důvodu nedostačující kapacity HFS. Limit systému se zvýšil na teoretických 8EB pro velikost jak jednoho souboru, tak i celého svazku. Apple představil toto vylepšení v roce 1998 s příchodem Mac OS 8.1. Od roku 2002 přibylo do systému souborů též volitelné žurnálování, které je identifikovatelné v typu svazku jako HFSJ.

HFS+ si fyzický disk rozdělí na logické bloky dlouhé 512 bytů, které dá do skupin logických bloků nazývaných alokační bloky. Mapa alokačních bloků je uložena ve speciálním souboru na počátku svazku – alokačním souboru (Allocation File). V alokačním souboru si systém udržuje informace o obsazenosti jednotlivých alokačních bloků. Záznamy o souborech a složkách jsou vedeny v B-stromu Katalogový soubor (Catalog File), kde se identifikují pomocí unikátního ID. Přiřazení alokačních bloků k souborům je evidováno v souboru Extents Overflow File, který má taktéž B-stromovou strukturu.

Princip mazání dat spočívá ve smazání záznamů z Catalog File a označení alokačních bloků za volné. Softwarové obnovení není sice nejjednodušší, ale speciální algoritmy toho jsou schopny.

3.2 Typy datových nosičů a princip ukládání dat

Zpracováno podle [2]

Pro ukládání počítačových dat se v průběhu let používalo mnoho různých nosičů lišících se kapacitou a velikostí ochranného obalu. Hlavním kritériem, jak rozdělit tyto nosiče, je způsob zápisu dat. Při odhlédnutí od nejstarších způsobů ukládání počítačových dat, jako byly děrné štítky, a také téměř nepoužívaných způsobů ukládání dat, lze tyto nosiče rozdělit na magnetické, optické a polovodičové úložiště.

3.2.1 Magnetická média

Magnetická média fungují na principu fyzikálního jevu – magnetismu, který se primárně projevuje silovým působením na pohybující se nabitá tělesa. V souvislosti s datovými médii jde hlavně o ferromagnetismus.

Ferromagnetismus, neboli jedna z nejsilnějších forem magnetismu, je výsledek fyzikálního a chemického složení feromagnetické látky. Materiály, které feromagnetismus vykazují, se vnitřně skládají z tzv. Weissových domén, což jsou „myšlené“ oblasti, kde jsou magnetické síly stejně orientovány. Pakliže na tyto materiály působí vnější magnetické pole, dojde ke sjednocení orientace magnetických momentů, tedy zesílení projevu magnetického pole samotné látky. Čím silnější bylo působení vnějšího magnetického pole, tím více je zesíleno vnitřní magnetické pole. Mezi feromagnetické látky patří zejména kobalt, železo, jejich slitiny a některé sloučeniny.

3.2.1.1 Pevný disk

Samotnou datovou částí jsou v pevných discích datové plotny. Nejčastěji používané velikosti datových ploten jsou 2,5 a 3,74 palce (3,74“ je skutečný rozměr oproti označení 3,5“). *Diskové plotny* jsou nejčastěji hliníkové, skleněné nebo keramické kulaté desky potažené tenkou vrstvou ferromagnetického materiálu, nejčastěji slitinou kobaltu jako

nosiče dat. Celý datový povrch je rozdělen na obrovský počet magnetických oblastí o velikosti asi 200-250 nm na délku a 25-30 nm na šířku (jedná se o údaje z roku 2006). Takováto oblast uchovává jeden bit informace, který dle směru magnetizace nabývá logické hodnoty 0 nebo 1. Dříve se využívalo podélného zápisu, ale ve snaze zvýšit hustotu dat se přešlo na kolmý zápis dat. Poslední hodnoty hustoty dat dosahují hodnot až 446 Gigabitů na čtvereční palec (Gbits/sq. In.), z čehož plyne maximální kapacita oboustranné diskové plotny „3,5“ disku“ jeden terrabyte (2^{40} bytů).

Samotné operace čtení a zápisu mají na starosti čtecí a zápisová hlava, které se pohybují těsně nad plotnami disku a převádějí magnetické pole na logickou informaci a naopak. Tyto hlavy jsou ovládány řídící elektronikou, která je zodpovědná i za komunikaci se samotným počítačem přes rozhraní, které je různé v závislosti na použití (domácí PC, servery).

3.2.1.2 Magnetické pružné disky

Jedná se o skupinu datových médií, která je již na ústupu. Tato média byla založena na velmi podobném principu jako pevné disky, s tím rozdílem, že podklad pod magnetickou vrstvou byl z pružného polymeru a mechanika pro čtení dat nebyla součástí datového média. Také se jako magnetické vrstvy často využívalo oxidů železa. Nejmarkantnější rozdíl je poté v hustotě zápisu dat, která je rozdílná o několik řádů. Dříve oblíbené Floppy disky už jsou dnes minulostí, kvůli jejich nespolehlivosti a malé kapacitě. Další zástupcem jsou ZIP disky, které nefungovaly o mnoho lépe i přes jejich větší kapacitu a spolehlivost.

3.2.1.3 Magnetooptické disky

Magnetooptické disky jsou občas řazeny do samostatné kategorie, případně mezi optické disky, ale jejich základní princip vychází z feromagnetických vlastností látek. Změny magnetizace domén je tu docíleno laserovým paprskem. Čtení pak probíhá na základě malé změny v lomu světla procházejícího různě zmagnetizovanou látkou (takzvaný Kerrův jev). Magnetooptické disky nejsou běžnou záležitostí, přesto však je lze dodnes najít v archivech některých institucí. Předností je poměrně slušná odolnost proti stárnutí – životnost bývá 100 let. Kapacita se dnes pohybuje v řádech gigabytů.

3.2.1.4 Magnetické pásky

Tento typ magnetického média stál u vzniku počítačového průmyslu a existuje už déle než 60 let. Moderní provedení je nejčastěji formou větších kazet. Jak už název napovídá, jedná se o pružnou pásku potaženou magnetickým materiálem. Struktura zápisu je lineární – tedy na šířce pásky je několik samostatných stop. Rychlost čtení moderních magnetických pásek je téměř na úrovni pevných disků, ale přístup k datům z různých částí je velice pomalý, protože závisí na rychlosti převinutí pásky na správné místo. Tyto důvody dělají z pásek ideální médium pro jednorázové zálohy dat, už jen z důvodu daleko nižší ceny při srovnatelné kapacitě oproti pevným diskům. Maximální kapacita jedné kazety se v posledních letech drží na úrovních maximálních kapacit pevných disků, tedy je dnes možno pořídit 5 TB (terrabyte) kazetu s magnetickou páskou.

3.2.2 Optická média

Nejrozšířenější optická média jsou kruhová s průměrem 12cm a 8cm. Nosný materiál je zpravidla polykarbonát. Nejsou citlivá na magnetické pole a otřesy. Základní princip je u všech stejný – používá laser pro čtení i zápis. Pro zápis dat se využívá takzvaných pitů, neboli malých dírek v reflexní vrstvě optického média. Odrazem laserového paprsku je poté algoritmy vyhodnocováno, zda se jedná o jedničku, či nulu. Optická média jsou aktuálně na ústupu.

3.2.2.1 První generace

První generace optických médií zahrnuje takzvaná CD (compact disc) neboli „cédéčka“ tedy disky s označením CD-ROM (read only memory), CD-R (recordable) a CD-RW (rewritable). CD-ROM je lisovaný typ s pevně danými daty, na ostatní typy je možno zapsat svá data a v případě RW je i přepisovat. První generace používá laser o vlnové délce 780nm. Média jsou pouze jednovrstvá. Standardní kapacita až 800MB dat.

3.2.2.2 Druhá generace

Druhou generací jsou DVD (Digital Versatile Disc) neboli „dévédéčka“. Využívají laseru o vlnové délce 640 nm. Datové stopy jsou mnohem blíže a menší, než tomu bylo u první generace. K dispozici jsou i dvouvrstvá média DL (double layer). Známé typy jsou DVD-ROM, DVD±R, DVD-RAM (random access memory), DVD±RW. V dvouvrstvém

provedení je kapacita 9,4GB dat. Označení + a – určuje dva mírně rozdílné standardy zápisu.

3.2.2.3 Třetí generace

Třetí generací optických médií se rozumí dvojice formátů HD-DVD a Blu-ray disk, z nichž komerčně úspěšný vyšel pouze Blu-ray. Modré laserové diody používají vlnovou délku 405 nm. Nejrozšířenější typy jsou BD-ROM, BD-R, BD-RE (rewritable). Standardní kapacita je 25GB na jednu vrstvu. Zpravidla se používá jedno a dvouvrstvová varianta, ale ve výrobě je i čtyřvrstvé médium.

3.2.3 Polovodičové paměti

Polovodičové paměti uchovávají data pomocí tranzistorů nebo stavů kondenzátorů. Pro uchovávání dat se využívají paměti nevolatilní, které uchovávají data i bez přísunu elektrické energie. Tyto paměti se v posledních letech nejvíce rozšiřují jako snadno přenositelná paměťová média.

3.2.3.1 ROM a další

ROM (Read Only Memory) je paměť používající unipolární tranzistory, které se nachází na průsečíku adresových linek X a Y. Stav tranzistoru otevřeno reprezentuje logickou hodnotu jedna a stav zavřeno logickou hodnotu nula. Vyznačují se velice rychlým přístupem k datům (10-20ns), ale data jdou zapsat jen jednou prostřednictvím masky. Velice podobně funguje typ PROM (Programmable Read-Only Memory), který je možné elektronicky naprogramovat, také pouze jednou. Hlavní rozdíl je v použití bipolárních tranzistorů. EPROM (Erasable Programmable Read-Only Memory) je opět unipolární typ paměti, který je možno opakovaně přepsat, ale mazání celého čipu probíhá například ultrafialovým světlem. EEPROM (Electrically Erasable Programmable Read-Only Memory) je elektricky mazatelná paměť s omezeným počtem přepisů, mazání probíhá přivedením kladného napětí na datové vodiče.

3.2.3.2 Flash EEPROM

Flash EEPROM je speciálním typem EEPROM, se změněnou vnitřní strukturou, s důrazem na dosažení maximální hustoty dat a minimální výrobní ceny. Tento typ paměti byl zkonstruován okolo roku 1980 doktorem Fujio Masuokou, když pracoval u firmy Toshiba. První komerční čip byl představen roku již 1988 společností Intel Corporation, navzdory tomu velký „boom“ zažívají tyto paměti až v posledním desetiletí. Známe dva hlavní podtypy a těmi jsou NAND a NOR, názvy se odvíjí od stejnojmenných funkcí booleovské algebry. Tyto paměti používají tranzistory s plovoucím hradlem. Data jsou ukládána do paměťových buněk, které jsou organizovány po blocích. V případě mazání nebo přepisu dat je třeba vymazat celý blok najednou. I tento typ paměti má pouze omezený počet přepisů předtím, než dojde k degradaci paměťových buněk, ale jedná se o čísla v řádech tisíců až statisíců. Právě tento typ paměti je používán v běžných paměťových kartách, jako jsou SD (Secure Digital), CF (CompactFlash), MMC (Multi Media Card), xD (xD-Picture Card). Dále se používá v různých USB flash discích, přenosných audio/video přehrávačích s vnitřní pamětí či v SSD discích. Zařízení složené z flash čipů může mít takřka libovolnou kapacitu, omezení vznikají jen na straně použitých řadičů. Aktuálně nejlepší vyráběné čipy mají kapacitu 16GB dat.

3.2.3.3 SSD disk

Přestože pro mnoho lidí může být SSD disk naprostou novinkou, první použití technologie flash disků sahá do sedmdesátých let. Společnosti IBM, Amdahl a Cray zavádějí tento druh paměti, ale vzhledem k neúměrně vysoké ceně se flash nedočká většího rozšíření. Až v roce 1978 uvedla společnost Texas Memory Systems moderní SSD paměti v podobě, jak je známe dnes. Jde o 16kB RAM SSD, které použily ropné společnosti pro jejich vysokou odolnost vůči vysokým teplotám a otřesům. V polovině osmdesátých let představila společnost Santa Clara BatRam 1MB DIP (Dual In-line Package) RAM čip s vlastním řadičem, který napodobil pevný disk. Balení zahrnovalo dobíjecí baterii pro uchování obsahu paměti v okamžicích, kdy paměť nebyla napájena systémem.

[11]

SSD (Solid-state drive) je typ datového média bez mechanických částí, které vyniká obzvláště v přístupu k náhodným datům, a dražší modely i výbornou rychlostí sekvenčního

čtení a zápisu. SSD se nejčastěji skládá z několika NAND flash pamětí zapojených paralelně. Je koncipován jako náhrada klasických pevných disků, a z toho důvodu emuluje rozhraní používané pro pevné disky. Vzhledem k omezenému počtu přepisů jednotlivých bloků je řadič SSD nucen zapisovat data pokaždé do jiných částí čipu.

Z důvodu informovanosti řadiče SSD o volných blocích byla s novými operačními systémy a SSD disky zavedena funkce TRIM, která informuje řadič o volných blocích. Jelikož před samotným zápisem je potřeba zapisované bloky „znulovat“, provádí si tuto činnost SSD disk v době nečinnosti a skutečně odstraňuje smazaná data. Tato podpora je však implementována pouze do Windows 7 a distribucí linuxu s verzí jádra vyšší než 2.6.33 spolu se souborovým systémem ext4. Mac OS má jen omezenou podporu pro „applovské“ SSD.

3.3 Metody bezpečného zničení dat

3.3.1 Algoritmy mazání dat

Způsoby neobnovitelného mazání disku softwarovou cestou byly řešeny mnoha světovými institucemi a konferencemi, důsledkem čehož byl vznik opravdu velkého množství standardů, respektive metod, kterými by se měly řídit minimálně státní instituce dané země. Na tomto místě jsou uvedeny alespoň některé z nich.

3.3.1.1 Standard DoD 5220.22-M

Standard DoD 5220.22-M je jedna z nejčastěji a nejvíce zmiňovaných metod. Paradoxem však zůstává, že její označení odkazuje na dokument organizace spadající pod ministerstvo obrany spojených států amerických NISP (National Industrial Security Program). Konkrétně se jedná o její o manuál NISPOM (NISP Operating Manual), ve kterém není ani zmínka o přesném způsobu mazání, jen obecně zdůrazněna potřeba zlikvidovat data bez možnosti obnovy. Standard uváděný pod tímto zavádějícím názvem zřejmě pochází z dokumentu agentury DSS (Defense Security Service), která taktéž spadá pod ministerstvo obrany spojených států amerických, s názvem „DSS Clearing and Sanitization Matrix“.

Možná ještě větší rozpaky vyvolává skutečnost, že ve verzi dokumentu DSS C&S Matrix z roku 2007, stejně tak jako v dalších, mladších verzích už je jakákoliv softwarová metoda likvidace citlivých dat pro magnetická média označena jako neakceptovatelná. Nicméně většina programů tuto metodu aplikuje následujícím způsobem: v prvním kroku je celé médium přepsáno logickými nulami, v druhém kroku se vše přepíše na jedničky a v posledním se celý disk přepíše náhodnými hodnotami. Důležitým bodem po každém průchodu je též verifikace alespoň 10% zapsaných hodnot.

3.3.1.2 Metoda „Peter Gutmann“

Metoda „Peter Gutmann“ byla poprvé publikována v červenci roku 1996 v dokumentu „Secure Deletion of Data from Magnetic and Solid-State Memory“. Vymyslel ji profesor Peter Gutmann společně s Colinem Plumbem na Univerzitě v Aucklandu (Nový Zéland). Jedná se o nejsložitější metodu ze všech používaných a mluví se o ní jako o nejbezpečnější metodě.

Tato metoda je sérií 35 přepisovacích cyklů s pevně danou strukturou. V průběhu prvních čtyřech průchodů jsou zapisovány náhodné hodnoty, následuje 27 průchodů se zápisem pevně daných vzorců, a série je zakončena opět čtyřmi průchody se zápisem náhodných dat. Z uvedeného jasně plyne, že se jedná o velice zdlouhavou a pomalou metodu a vyčistění jednoho gigabytu dat může při nejčastěji uživateli reportované rychlosti okolo 5Mb/s trvat až dvě hodiny. Pro smazání dnes poměrně běžného 1TB (reálně cca 930GB) disku by tedy bylo potřeba počítat s přibližnou dobou trvání neuvěřitelných 75 dní.

3.3.1.3 Ruský GOST R 50739-95

„GOST R 50739-95“ je označení normy pocházející ze souboru norem známých pod názvem GOST, který má na starosti Euroasijská rada pro normalizaci, metrologii a certifikaci (EASC). Tyto normy jsou používány v zemích bývalého Sovětského svazu. Metoda bývá nejčastěji implementována jako dvouprůchodová. V prvním průchodu jsou na paměťové médium zapsány pouze nuly a v druhém průchodu jsou zapsány náhodné znaky.

3.3.1.4 Britský HMG Infosec Standard 5

Britský „HMG Infosec Standard 5“ je metoda zakotvená v britských dokumentech „Security Policy Framework“, které zpracovala skupina CESG (Communications-Electronics Security Group), která je součástí britské výzvědné služby „Government Communications Headquarters“. Tato metoda je tří průchodová s verifikací po každém kroku. V prvním kroku se přepíšou data na samé nuly, v druhém kroku na samé jedničky a v třetím jsou zapisovány náhodné znaky. Výsledná verifikace musí ověřit, že jediné, co lze z datového média přečíst, jsou náhodné znaky.

3.3.1.5 Kanadský RCMP TSSIT OPS-II

RCMP TSSIT OPS-II je metoda mazání dat používaná královskou kanadskou jízdní policií (Royal Canadian Mounted Police). Metoda je stále oblíbená a do programů často implementovaná navzdory tomu, že od ní už RCMP ustoupilo. Celý algoritmus sestává ze sedmi průchodů. V průběhu prvních šesti přepisů se střídá zápis pouze nul a jedniček, tedy sekvence 0,1,0,1,0,1. V posledním přepise se zapíše náhodný znak, a je verifikováno jeho zapsání.

3.3.1.6 Německý VSITR standard

Německý „VSITR standard“ je metoda standardizovaná Německým spolkovým úřadem pro informační bezpečnost (BSI - Bundesamt für Sicherheit in der Informationstechnik). Jedná se o metodu téměř identickou s RCMP TSSIT OPS-II. Jediným rozdílem je, že v posledním kroku není vyžadována verifikace zapsaných dat.

3.3.1.7 Algoritmus Bruce Schneiera

Tento algoritmus byl vymyšlen americkým kryptografem a odborníkem na počítačovou bezpečnost Brucem Schneierem, který jej publikoval roku 1994 ve své knize "Applied Cryptography: Protocols, Algorithms, and Source Code in C" (ISBN 9780471597568). Algoritmus je implementován jako sedmiprůchodový. V prvním kroku se celý datový prostor přepíše jedničkami a v druhém kroku nulami. Následujících pět průchodů je datové médium přepisováno pseudonáhodnými hodnotami. Pseudonáhodné hodnoty si lze představit jako posloupnost hodnot, které se zdají být na první pohled zcela náhodné, ale ve skutečnosti jsou vygenerovány deterministickým algoritmem.

3.3.1.8 Rychlé metody

Do této skupiny spadá mnoho rychlých metod založených na jednom přepisu a zároveň bez verifikace přepsaných hodnost. Jedná například o metodu „Fast Zero“ někdy nazývané též „Write Zero“ – přepis nulami nebo „Random Data“ přepis pseudonáhodnými hodnotami. Existují i metody, které nepřepisují celý datový prostor, ale pouze náhodně rozsévají řetězce hodnot, aby došlo k poškození původních dat. Jedinou výhodou těchto metod je jejich rychlost v porovnání s víceprůchodovými metodami.

3.3.2 Výhody a nevýhody softwarových metod

Nyní jsou uvedeny výhody a nevýhody nasazení softwarových přepisovacích metod. Na prvním místě budou představeny výhody. Za hlavní výhodu lze označit zachování média, tedy možnost jeho znovu použití anebo zpeněžení. Softwarovými metodami lze taktéž čistit data na vzdálených počítačích a úložištích. Další nespornou výhodou softwarových metod je možnost těchto programů udělat textový, či datový výstup o vyčištěných médiích, což usnadňuje evidenci vyčištěného hardwaru a může sloužit i jako doklad o likvidaci. Oproti tomu nevýhodou je nemožnost použití těchto metod na poškozené nosiče, které ovšem poškozením neztratily data. V praxi to znamená například poškození mechanismu ovládání harddiskových hlaviček. U některých typů magnetických pamětí je též riziko rekonstrukce původních dat, zvláště při použití jednoduchých metod. Více v kapitole „Obnova smazaných dat“.

3.3.3 Fyzikální metody zničení dat

Kromě softwarových poměrně pomalých metod, jak odstranit data, jsou tu i fyzikální možnosti likvidace dat. Většinou se jedná o velice rychlé metody, ale nevýhodou zůstává, že datové medium už nebude možné znovu použít, případně zpeněžit. Pro média založená na magnetickém zápise, tedy magnetické indukci, se v profesionálních firmách zabývajících se ničením dat používá nejčastěji magnetizace a pro jiný typ médií fyzické poškození úložiště.

3.3.3.1 Magnetizace

Naprostá většina dnes nejpoužívanějších běžných datových úložišť využívá magnetického zápisu. Ze způsobu zápisu proto plyne i možný způsob zničení datového obsahu těchto médií. Magnetizace je proces, respektive fyzikální jev, ke kterému dochází při vložení tělesa do silného magnetického pole. V tomto případě se jedná nejčastěji o feromagnetický materiál s magnetickým dipólovým momentem, který se po vložení do silného magnetického pole zorientuje stejně podle siločar magnetického pole, do kterého byl vložen. Tímto zmizí logická reprezentace jedniček a nul, jakožto opačných a přesně orientovaných magnetických sil.

Moderní pevné disky mají mnohem lepší stínění, než tomu bylo v dřívějších dobách, a proto je vyžadováno o mnoho silnější magnetické pole. Bohužel z toho vyplývá, že není žádná záruka zničení všech dat zvláště u starších strojů na magnetizaci disků, což znamená zvýšené bezpečnostní riziko. Není však možné (v běžných podmínkách) ani ověřit, zda došlo ke kompletnímu vymazání, protože v silném magnetickém poli jsou poškozeny i další části pevného disku, který se již nikdy neroztočí. Na druhou stranu, u hůře chráněných datových médií, jako jsou diskety nebo magnetické pásky, postačí i daleko menší magnetické pole a tyto média mohou být bez problému likvidována i v domácích podmínkách.

Specializované profesionální stroje na likvidaci magnetickým polem jsou také velice drahé a tím pádem pro domácího uživatele a lze říct i menší firmy nedostupné a nerentabilní. Další nevýhodou těchto strojů je nutnost držet od nich v dostatečné vzdálenosti jakékoliv vybavení elektrotechnického charakteru, aby nedošlo k jeho poškození.

Nyní bude tato metoda posouzena a z hlediska výhod a nevýhod. Za výhodu lze považovat tyto schopnosti: zničit všechna data naráz, možnost ničení všech možných typů magnetických médií, dále je nutno uvést, že magnetizace je velice rychlý proces, kromě toho pořízení specializovaného stroje je jednorázovou investicí. Oproti tomu nevýhody jsou tyto: u moderních pevných disků není stoprocentní jistota zničení všech dat a díky zničení více částí pevného disku není možné zničení všech dat ověřit. Dále se datové médium stává nepoužitelným a tím pádem ztrácí veškerou hodnotu, není možné likvidovat jiné typy datových nosičů. Jako další je nutno uvést vysokou pořizovací cenu

profesionálního stroje, a v případě využití služeb specializovaných firem se klient vystavuje riziku neprofesionálnosti těchto firem a jejích pracovníků, tedy a možnému datovému úniku.

3.3.3.2 Fyzická destrukce

Kromě již zmíněných metod existují i metody založené na destrukci a poškození datového média za účelem jeho totální nečitelnosti. Tyto metody většinou představují nejjistější a velice efektivní cestu, jak se zbavit citlivých dat. Avšak představují také zvýšené zdravotní riziko plynoucí z odletujících kousků materiálů ničeného média, případně manipulací s nebezpečnými látkami. Je třeba také poznamenat, že většina těchto metod neodstraní data samotná, ale způsobí, že je nemožné rekonstruovat ze zbytků datového média jakoukoliv relevantní část dat. Různých metod se dá najít opravdu nespočet a téměř se dá říci, že se fantazii meze nekladou. I na tyto metody existují speciální stroje, které většinou fungují na principu úplného rozdrcení materiálu.

Dalšími pomocníky bývají obyčejná vrtačka a kladivo. Vrtačka se v případě ničení pevného disku používá k navrtání dostatečného počtu otvorů do ploten disku, až dojde k jejich úplnému rozpadu. V případě SSD disků je to podobné, ale je nutné navrtat každý jednotlivý paměťový čip. Pokud se někdo rozhodne využít kladiva či palice, je ničení SSD a flash disků ještě rychlejší, ovšem u harddisku je nutné demontovat horní ochranný kryt. K urychlení zničení pevného disku pomocí kladiva se využívají více či méně speciální prorážedla.

Dále se zvláště u nekovových datových nosičů využívá technik, jako je broušení, tavení, případně kompletní spalovaní. K chemické likvidaci se přistupuje spíše výjimečně a poté se využívá konkrétních chemických vlastností médií a za pomocí například kyseliny je narušen samotný datový materiál – tedy nemusí dojít k rozpuštění celého nosiče. K ničení plastových ROM médií se nezřídka využívají i skartovačky na papír.

Dříve se také využívaly specifické vlastnosti feromagnetických látek, to je ztráta magnetického momentu po přesažení určité teploty. Teplotní bod, nad kterým zaniká magnetický projev, se nazývá Curierova teplota. Avšak reálné použití na dnešní pevné disky je značně spekulativní, protože pro datovou vrstvu nejčastěji používaná slitina kobaltu má velmi vysokou Curierovu teplotu. Samotný kobalt má Curierův bod v 1000 °C,

což je ale daleko za teplotou tání hliníku (660 °C), který je nejčastějším obalem pevných disků a zároveň i nosným materiálem samotných ploten disku.

Obrázek 1 – Pevný disk po fyzické likvidaci „http://www.hughestechnologiesinc.com/Portals/0/Hard-Drive-Destruction.gif“

3.3.3.3 Výhody a nevýhody fyzických metod

Z hlediska posouzení výhod a nevýhod těchto metod se za výhodu dá považovat možnost ničení mnoha médií najednou. Dalšími výhodami jsou: možnost kombinovat typy médií, rychlost a efektivita zničení dat zvláště oproti softwarovým metodám. Nevýhodou pak je úplné znehodnocení datového média a nemožnost jeho opětovného použití, a dále určité menší riziko, že zvláště u „ručních“ metod nebude vše dostatečně rozbito a některé fragmenty dat bude možné přečíst a zneužít.

3.3.3.4 Stroje na poškození a zničení datových médií

Nyní jsou uvedeny některé konkrétní typy strojů na ničení dat, v prvé řadě stroj založený na magnetizaci a dále stroje založené na fyzické likvidaci.

Garner TS-1 Data Eliminator

Tento stroj je schopen smazat jakékoliv magnetické médium magnetickým polem dosahujícím síly 2 Tesla (20,000 Gaussů). Stroj je opatřen certifikací NSA/CSS/DoD Top Secret, tedy splňuje požadavky Ministerstva obrany Spojených států amerických a jeho podřízených agentur. Jeden mazací cyklus trvá 45 vteřin a je hlídán senzory síly magnetického pole. Všechny chybové hlášky jsou zobrazeny na malém LCD panelu.

Prostor pro magnetizaci na rozměry (výška, šířka, hloubka) 2.54*11.43*17.15 cm, tedy je možné magnetizovat jakékoliv médium, které se vejde do tohoto prostoru.

Obrázek 2 – Garner TS-1 Data Eliminator
http://www.garnerstore.com/media/catalog/product/cache/35/image/9df78eab33525d08d6e5fb8d27136e95/g/a/garner-ts-1-nsa-hard-drive-and-tape-degausser.jpg

SEM Model 0301 Jackhammer Hard Drive Shredder

Drtič od firmy SEM (Security Engineered Machinery) je představitelem fyzické likvidace, konkrétně se jedná o metodu drcením. Vyznačuje se rychlostí a silou drcení. Je schopen rozdrtit veškeré pevné disky do tloušťky 4.2 cm rychlostí 2000 pevných disků za hodinu. Motor o síle 3,7 kW pohání drticí čelisti, které rozdrtí harddisk na malé kousky velké maximálně 3,8cm šířky. Nevýhodou jsou ovšem velké nároky na prostor, a to jak samotného stroje, tak odpadního koše.

Obrázek 3 – SEM Model 0301 Jackhammer
http://www.trendshredders.com/product_images/p/524/jackhammer_0301_350px__11449_zoom.png

Garner PD-4 Physical Hard Drive Destroyer

Jedná se o poměrně malý a mobilní stroj pracující na základě lámání a ohýbání a lisování. V případě pevných disků jsou veškeré vnitřní části poškozeny a datové plotny rozlámány. Celý proces trvá 20 vteřin a je možné ničit dva pevné disky naráz. Doporučené je též zkombinovat s nějakým demagnetizérem pro úplnou jistotu zničení všech dat.

Obrázek 4 – Garner PD-4 http://www.garner-products.com/images/HD-After-PD-4Crush.jpg

3.4 Důležitost mazání dat

Elektronická data v rukách nesprávné osoby představují velké nebezpečí. Přesto se ne vždy podniká dost pro to, aby v nich neskončila. Příkladem neopatrného nakládání s daty je jejich mazání. Zatímco u tištěných dokumentů je třeba rozhodnout, zda skončí v odpadkovém koši nebo ve skartovacím zařízení, elektronická data, ať jsou citlivá či nikoli, jsou většinou mazána tímtéž způsobem. Přitom smazané informace je možné velmi jednoduchým způsobem vrátit do původního stavu. Nejde o pouhé obnovení dokumentu z odpadkového koše ve Windows.

[12]

3.4.1 Citlivé údaje

Zpracováno dle § 4 zákona č. 101/2000 Sb., o ochraně osobních údajů *[8]*

Z hlediska legislativního se jedná o osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových

organizacích, náboženství a filozofickém přesvědčení, trestné činnosti, zdravotním stavu a sexuálním životě subjektu. Osobním údajem se potom rozumí jakýkoliv údaj týkající se určitého subjektu. Subjektivní údaj je pak považován za určitý, jestliže lze na jeho základě přímo, či nepřímo zjistit identitu subjektu.

Z hlediska utajení pak informace dělíme na přísně tajné, tajné, důvěrné nebo vyhrazené. K jednotlivým stupňům se pak váže konkrétní ochrana i způsob likvidace.

3.4.2 Význam pro domácí uživatele i podniky

Pro samotné uživatele pak platí „zlaté“ pravidlo, že reálná hodnota dat bývá jejich vlastníkem doceněna až při jejich neautorizovaném využití, zničení nebo momentální, či trvalé nedostupnosti. Zneužitelnými daty se může stát téměř cokoliv, počínaje výběrem hudby, přes audio/video nahrávky, fotografie až po samotné dokumenty a hesla. Běžný uživatel má na pevném disku uloženy desítky přístupových údajů a mnohdy si to ani neuvědomuje. Všechna tato data mohou být při neopatrném jednání obnovena z vyhozených, darovaných, či prodaných pevných disků.

V případě podniků je nutno posuzovat ztrátu dat podle možného negativního dopadu na společnost. Musí se zvážit, jaké škody mohou vzniknout v případě odcizení a následného zneužití. Únik firemních informací může mít za následek ztrátu pozice na trhu, ztrátu důvěryhodnosti a z toho plynoucí ztrátu tržeb. Únik informací může být vyvolán i cílenou akcí – takzvanou podnikovou špionáží.

3.5 Legislativa a hrozící trest

Legislativa ochrany dat a s ní spojené úniky se v České republice zaměřuje zvlášť na ochranu osobních údajů. Celá legislativa vychází z Listiny základních práv a svobod. Článek 10 zaručuje ochranu před neoprávněným zneužitím osobních údajů a článek 13 zaručuje tajemství uchovávaných záznamů a písemností. Podrobnější úprava je potom řešena hlavně zákony: Zákon č. 101/2000 Sb., Zákon o ochraně osobních údajů, Zákon č. 40/1964 Sb., občanský zákoník (ochrana osobnosti) a Zákon č. 40/2009 Sb., nového trestního zákoníku.

Zákon č. 40/2009 Sb., trestní zákoník

§ 180 Neoprávněné nakládání s osobními údaji

(1) Kdo, byť i z nedbalosti, neoprávněně zveřejní, sdělí, zpřístupní, jinak zpracovává nebo si přisvojí osobní údaje, které byly o jiném shromážděné v souvislosti s výkonem veřejné moci, a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají, bude potrestán odnětím svobody až na tři léta nebo zákazem činnosti.

(2) Stejně bude potrestán, kdo, byť i z nedbalosti, poruší státem uloženou nebo uznanou povinnost mlčenlivosti tím, že neoprávněně zveřejní, sdělí nebo zpřístupní třetí osobě osobní údaje získané v souvislosti s výkonem svého povolání, zaměstnání nebo funkce, a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají.

(3) Odnětím svobody na jeden rok až pět let, peněžitým trestem nebo zákazem činnosti bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 nebo 2 jako člen organizované skupiny,

b) spáchá-li takový čin tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem,

c) způsobí-li takovým činem značnou škodu, nebo

d) spáchá-li takový čin v úmyslu získat pro sebe nebo pro jiného značný prospěch.

(3) Odnětím svobody na tři léta až osm let bude pachatel potrestán,

a) způsobí-li činem uvedeným v odstavci 1 nebo 2 škodu velkého rozsahu, nebo

b) spáchá-li takový čin v úmyslu získat pro sebe nebo pro jiného prospěch velkého rozsahu.

[9]

Nakládání s utajovanými informacemi pak upravuje VYHLÁŠKA č. 523/2011 Sb. Národního bezpečnostního úřadu, která řeší i certifikace strojů pro skartaci a ničení tajného materiálu a bezpečnost informačních systémů.

Finanční postihy za menší provinění hrozí do 100 000 Kč, za větší unik a zneužití osobních informací až 5 000 000Kč. Správci dat jakožto instituci pak hrozí pokuta až 20 000 000Kč. Tyto pokuty vyměřuje Úřad pro ochranu osobních údajů.

V rámci mezinárodních vztahů pak ČR přistoupila k implementaci direktivy 94/46/EC Evropské komise, pracující pod záštitou Evropské Unie. Tato direktiva byla zapracována právě jako Zákon č. 101/2000 Sb., Zákon o ochraně osobních údajů. Jsou v něm definována pravidla pro zpracování a výměnu citlivých osobních dat mezi státy EU.

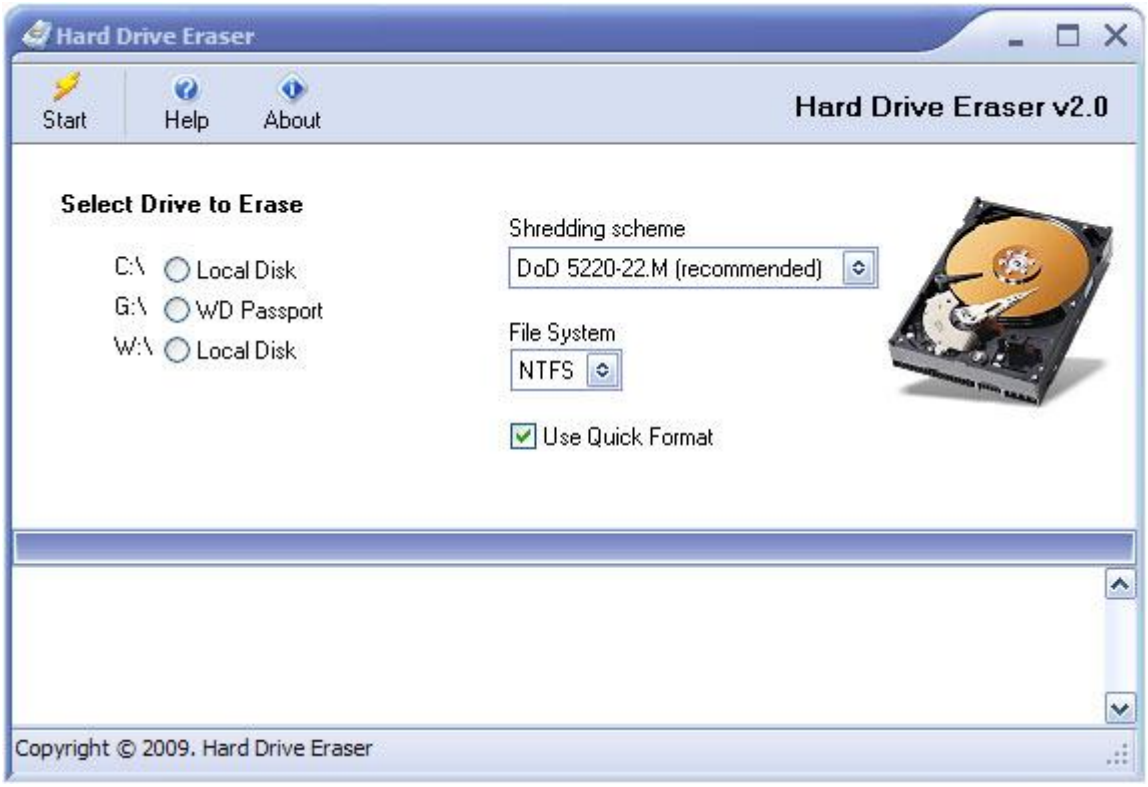
Ochrana firemních informačních dat jako takových není legislativně ošetřena. V některých zemích, jako jsou Spojené státy americké (USA), se legislativa vztahuje i na tyto případy, a je tvrdě postihován jakýkoliv únik firemních dat. Podle „Sarbanes–Oxley Act of 2002“ hrozí za únik finančních dat až 20 let vězení a pokuta do 5 000 000 USD. Organizace jsou často nuceny mít důkazy o provedeném zničení dat a jsou svazovány různými standardy.

3.6 Software pro bezpečné mazání dat:

Existuje obrovské množství různých softwarů pro bezpečné mazání dat. Výběr představeného softwaru byl sestaven na základě průzkumného dotazníku mezi uživateli počítačů (kapitola 4.7), kde byl dále uvedený software nejčastěji zmiňovaný.

3.6.1 Hard Drive Eraser

Hard Drive Eraser je malý jednoduchý program šířený jako svobodný software pod licencí GNU General Public Licence, jehož nasazení je možné jen pod systémy Windows. Program je optimalizován na jednoduchost ovládání a pro rychlost bezpečného mazání. Podporované souborové systémy jsou však také pouze spjaté se systémy Windows, tedy jedná se o FAT, FAT32 a NTFS. Pokud se jedná o implementované metody, byly implementovány celkem čtyři, jedná se o „Write Zeros“, standard DOD 5220-22.M, US Army a metoda „Peter Gutmann“. (samostatně vysvětleno v kapitole 3.2.1.2) Poslední uvolněná verze je verze 2.0, která je velká pouhých 618 kB. Tento jednoduchý a nijak certifikovaný program se dá označit za naprosto dostatečný v případě skutečného přepsání všech dat.



Obrázek 5 – Hard Drive Eraser
„http://www.harddriveeraser.org/images/screenshot_big.jpg“

Je vhodné též poznamenat, že některé operační systémy si vystačí se systémovými nástroji a dokážou přepsat celá datová média náhodnými hodnotami, případně nulami. Například v unixových systémech si lze pomoci speciálními systémovými soubory /dev/zero, /dev/random a /dev/urandom. Soubor /dev/zero generuje nulové hodnoty a /dev/random a /dev/urandom náhodné hodnoty, jediný rozdíl je v použití entropie a rychlosti, kde vychází lépe /dev/urandom. Poté jen stačí využít těchto souborů a „nakopírovat“ je na cílové médium. Samotná syntaxe je pak například:

dd if=/dev/zero of=/dev/sda

cp /dev/zero /dev/sda

cat /dev/zero > /dev/sda

4 Obnova smazaných dat

4.1 Datová remanence

Na začátku je třeba definovat pojem takzvané. „datové remanence“. Jde o zbytkový pozůstatek smazaných dat, která byla smazána jen obyčejně „nalehko“ – vyřazena z tabulky souborů. Jde o jev, kdy reziduální reprezentace dat zůstává na disku i po pokusech o vymazání dat. Zároveň jde o potencionální riziko nechtěného úniku citlivých dat do neznámých rukou.

Datová remanence je nejčastěji spojována s magnetickými typy paměti, ale lze ji nalézt i u dynamické RAM (random access memory), kde zůstávají data i po odpojení přívodu elektrické energie po několik málo sekund, v případě extrémního podchlazení dokonce i několik minut. Jak je uvedeno dále, formátování ani nové rozdělení disku nezaručuje neobnovitelnost předchozích dat. Také díky anti-fragmentačním technologiím mohou „neviditelné“ kopie mazaných dat fyzicky stále existovat na jiných místech pevného disku, aniž by o tom byl uživatel informován.

4.2 Záchrana dat

Záchrannou dat se zabývá široká škála firem, kde se používají různé softwary a o trochu jiné metody. Především se zabývají obnovou dat na pevných discích. Mnoho chyb médií a jejich mechanik může způsobit fyzické poškození záznamového média. V případě optických disků to může být například poškrábaná vnější vrstva nebo sloupnutá odrazová vrstva. Pevné disky mívají pak spálené motorky, zadřená ložiska, spálené řídící obvody nebo poškrábané plotny vinou doteku s hlavičkami. U magnetických pásek je to pak nejčastěji zmačkání nebo přetržení. USB Flash paměti pak mívají ulomené konektory nebo spálené řadiče. Většinu těchto problémů si nemůže běžný uživatel opravit sám, a proto je svěřuje do rukou odborníkům. Fyzické poškození ve většině případů vede ke ztrátě nějakých dat, ale zbytek bývá obnovitelný. Pokud je paměť poškozena na logické rovině,

tak je nejprve nutné napravit logické chyby a pak se mohou zkopírovat samotná data. Často se jedná o zhroucený souborový systém, vadný diskový oddíl anebo chyby média.

Obnova dat z fyzicky poškozeného hardwaru zahrnuje mnoho zajímavých technik. Někdy stačí vyměnit vadný díl a zpřístupnit tak data pro záchranu speciálními softwary, které udělají bitový obraz disku. Tento obraz se pak může zanalyzovat na logické chyby plynoucí z fyzického poškození a je z něj rekonstruován souborový systém a kopírována data.

Poměrně složitou metodu pak představuje záchrana dat při specificky poškozené ovládací elektronice disku, kdy je z jednoho pevného disku odpojena elektronika za běhu a stále pod proudem je připojena do poškozeného disku. V případě zadření, či selhání motorku jsou pak v bezprašném prostředí prohozeny plotny do jiného pevného disku typově shodného s původním.

Problémy logického rázu pak mohou být přepsaná data, omylem, či cizím zaviněním, smazaná data, a jakékoliv poškození souborového systému. Pokud jsou data přepsána na běžném pevném disku, tak se ve většině případů jedná o nenávratnou ztrátu, někdy se dají obnovit jen fragmenty.

V případě SSD disků, bez funkce TRIM (vysvětleno v kapitole 3.3.3.3), je šance, že i po přepisu logického prostoru se data nachází stále fyzicky na čipech, díky logice SSD disků, která přiřazuje logický prostor pokaždé jinému fyzickému prostoru. Tento jev dává poté prostor specializovaným technikám prohledat celý fyzický prostor a zkopírovat z něj veškerá dostupná data.

Pokud se jedná o problém se souborovým systémem, pak se záchrana provádí pokusem rekonstruovat tento systém pomocí doplnění, či úpravy tabulky rozdělení disků, či tabulky souborů. Je zde i možnost najít stínové kopie tabulky souborů a pokusit se obnovit tuto byť starší verzi. V případě logického poškození se v poslední době prosazuje i takzvaná „Online záchrana dat“, kdy se technik ze specializované firmy připojí vzdáleně k lokálnímu počítači a rovnou se pokusí obnovit data.

4.3 Laboratorní metoda MFM

MFM (magnetic force microscopy) nebo česky mikroskopie magnetické síly je laboratorní technika určená k získání magnetického prostorového obrazu s vysokým rozlišením. Tato technika byla odvozena z SPM techniky (scanning probe microscopy). V průběhu několika posledních let se MFM vyvinula z čistě výzkumného nástroje na široce používanou mikro-magnetickou zobrazovací techniku. Zjednodušeně jde o ostrý magnetický hrot potažený několika vrstvami magnetickým látek. Hrot je upevněný na raménku a spolu dohromady tvoří sondu, která se pohybuje těsně nad povrchem (desítky až stovky nanometrů) a magnetickou interakcí mezi vzorkem a hrotem dochází k výchylkám celého raménka, které jsou pak nejčastěji opticky detekovány a zapisovány formou průběžného grafu. Prezentace zachycených dat pak může být jako 3D model povrchu.

Touto metodou tedy mohou být bez problému přečtena všechna aktuálně zapsaná data na jakémkoliv magnetickém povrchu, ale je zde i možnost zjistit předchozí zapsaná data. Problém je ve skutečnosti v zápisu samotných dat, zápisová magnetická hlava při zápisu změní polaritu pouze většiny magnetických domén, a ne všech domén, což je způsobeno malými nepřesnostmi nastavení zapisovací hlavy nad magnetickou stopou, a také to záleží na síle magnetického pole, kterým působí omezeně tak, aby nezmagnetizovala i okolní domény. Princip zjišťování předchozího stavu magnetický domén funguje na základě zjištění přesné hodnoty magnetického pole nad každou z domén. Po prvním zápisu je hodnota magnetického pole každé z domén na celé plotně zhruba stejná a dá se označit jako hodnota 1. Orientace tohoto pole pak určuje logické hodnoty. Přepisuje-li se toto pole stejnou logickou hodnotou, dojde k zesílení původního magnetického pole na hodnotu, která ve vztahu k původní hodnotě jedna je o 5% vyšší. Tedy 1.05 původní síly magnetického pole. Naopak přepisuje-li se magnetické pole opačnou logickou hodnotou, pak je nové magnetické pole o něco nižší než bylo nominální. Tato hodnota je asi o 5% nižší, tedy 0,95 původní síly magnetického pole.

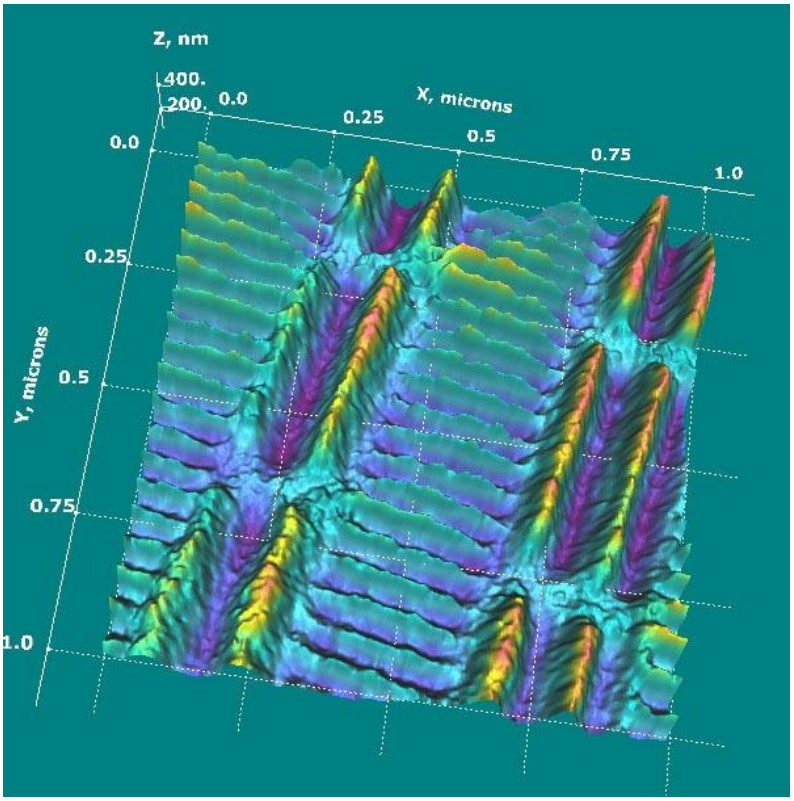
Tento stav magnetickým médiím nevadí, protože řídící logika vyhodnocuje nuly a jedničky v širším rozsahu, než je ideální stav magnetického pole. Ovšem pokud tato data přečteme pomocí MFM, tak na grafu vidíme i ty nejmenší odchylky a pomocí algoritmů není problém „přečíst“ aspoň dvě vrstvy původních nepřepsaných dat. Množství přepisů,

po kterých ještě lze dopočítat původní data, je omezeno velikostí magnetických stop čteného média a přesností čtecího zařízení.

Obnovení dat touto metodou analyzoval novozélandský vědec Peter Gutmann a na základě studie magnetických přepisů navrhl metodu mazání dat, po které není možné zjistit původní obsah. (více kapitola 3.2.1.2) Realita je však taková, že nejsou žádné důkazy o obnovení celého vícekrát-přepsaného pevného disku pomocí MFM. Tato metoda je nejúčinnější pro média, jako jsou floppy disky a starší magnetické pásky.

Rekonstrukce dat na moderních pevných discích byla mnohými vědci považována za fámu, a proto odborník na forenzní analýzu dat Craig Wright a jeho kolegové prozkoumali možnosti rekonstrukce dat pomocí MFM. Své výsledky pak prezentovali na mezinárodní konferenci ICISS 2008 (International Conference on Information Systems Security) pod názvem „Overwriting Hard Drive Data: The Great Wiping Controversy“. [10]

Ze studie vyplývá, že stačí přepsat moderní pevný disk čímkoli a stará data jsou nenávratně ztracena. Prakticky všechny pevné disky vyrobené po roce 2000 mají datové stopy tak blízko sebe, že ani pokrok v MFM nedokáže přečíst magnetickou stopu s dostatečnou přesností. Jedinkrát přepsaný bit byl rekonstruován s přesností 56 procent a k přečtení celého bytu bylo třeba osmkrát opakovat čtení, a pravděpodobnost správného výsledku byla pouhých 0.97 procent.



Obrázek 6 – 3D MFM obraz plotny pevného disku
http://www.sciencegl.com/3Dsurf/Shots/HD_mAFM1.jpg

4.4 Šifrování dat

Jako ochrana dat proti zneužití a tím pádem pomocník při bezpečném mazání dat může též sloužit i šifrování dat. Šifrování dat je jistým druhem vědního oboru kryptografie a zabezpečuje zašifrovaná data proti zneužití.

Hlavním úkolem kryptografie je zajištění důvěrnosti chráněných dat. Nikdo nepovolaný nesmí mít možnost přečíst data, která jsou chráněna kryptografickými prostředky, a to ani po vyvinutí jistého úsilí, nasazení vysoce výkonných výpočetních systému či týmu odborníků.

[1]

Vhodné je mít zašifrovány aspoň dokumenty, hesla, přihlašovací údaje a jiné citlivé údaje. Šifrování zamezí přístupu k datům i v případě fyzické ztráty média a zamezuje

využívání datové remanence. Zjednodušeně se jedná o proces, kdy se samotná data pomocí složitých algoritmů a klíče promění v data šifrovaná. Možností šifrování je velké množství, ale velice důležitý je pak i šifrovací klíč a silné heslo. Existuje možnost šifrovat jednotlivá data – potom jde o souborové šifrování. Další možností je šifrování celého disku, kdy nějaký program vytváří transparentní vrstvu pro komunikaci mezi fyzickým diskem a aplikacemi a stará se o šifrování a dešifrování dat. Takovýto program většinou pracuje s virtuálním diskem, který je na nešifrovaném disku prezentován jako jeden velký soubor – takzvaný kontejner. V praxi to pak funguje tak, že bez správného klíče a hesla se nenastartuje ani systém. Nevýhodou pak je ztráta určité části výkonu počítače a pomalejší datové přenosy.

Samozřejmě existuje i věda zvaná kryptoanalýza, zabývající se získáním obsahu takto zašifrovaných dat. Úspěšnost těchto pokusů o takzvané prolomení kódu zjednodušeně klesá se složitostí algoritmů a uživatelského hesla. A obzvláště z pouhých fragmentů dat je obtížné dešifrovat jakýkoliv smysluplný záznam. Samozřejmě, nic není naprosto stoprocentní a lidský faktor v tom hraje významnou roli.

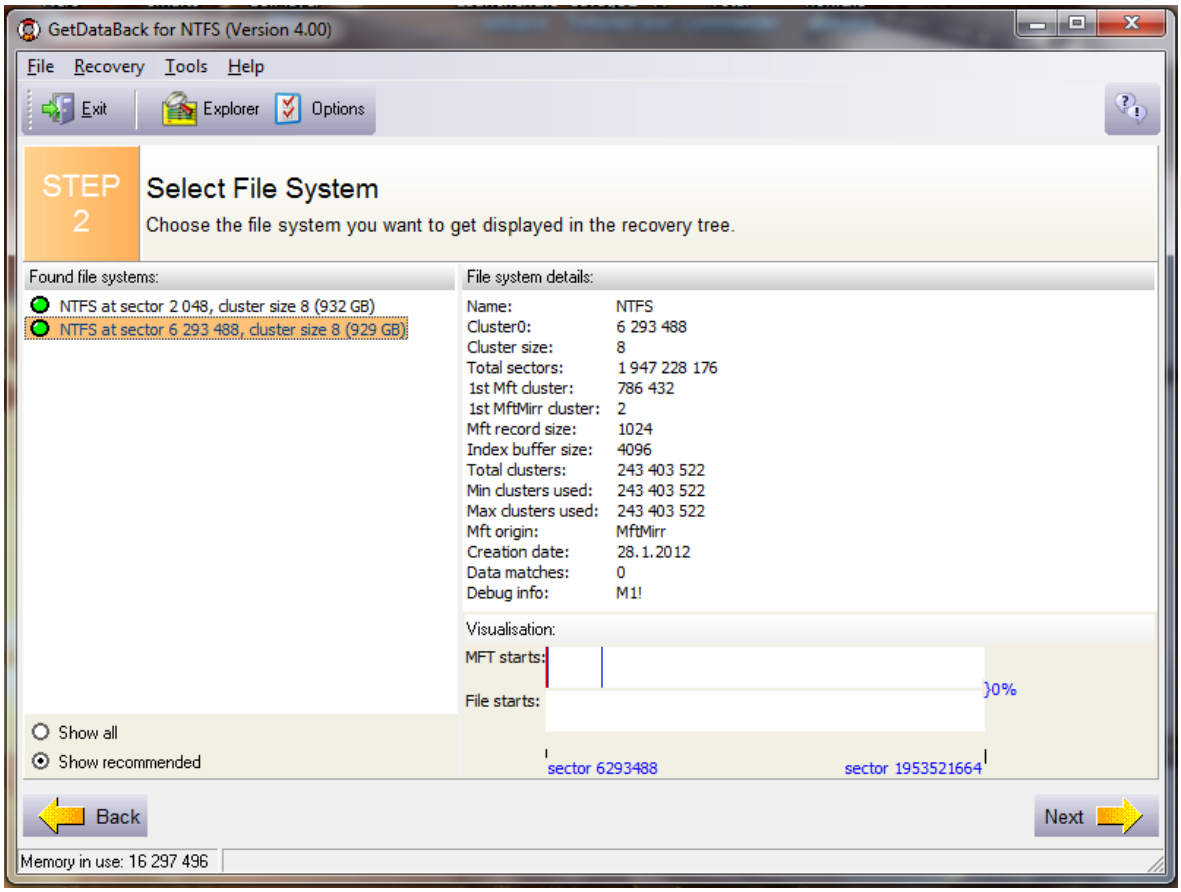
4.5 Software pro obnovu dat:

Pro softwarové metody obnovy dat je k dispozici mnoho převážně komerčních aplikací, které už se skutečně liší ve své efektivitě a úspěšnosti obnovy dat. Zde je uveden program, jenž je široce uznáván pro svoje schopnosti a je využíván i v některých firmách specializujících se právě na záchranu dat.

4.5.1 GetDataBack

Software GetDataBack je programem ze série programů pro nízko-úrovňový přístup k pevným diskům a úložištím americké společnosti Runtime Software. Tento program je dostupný ve verzích pro FAT32 a NTFS, poslední verze je V4.25 dostupná za $69 respektive $79 USD. K dispozici je také omezená zkušební verze. Analýza disku je velice detailní a program používá vlastní algoritmy, které skenují jednotlivé sektory a sestavují z nich fragmenty souborů. Program dbá na to, aby na analyzovaný disk nic nezapisoval, ale pouze z něho četl, což je základním principem každého kvalitního softwaru na obnovu dat. Program umí opravit MFT, FAT a MBR, dokáže zobrazit i přesné

(sektorové) umístění těchto tabulek a jejich kopie. Dále je schopen obnovit smazaná data, případně jejich fragmenty, i v případě, že byly některé části přepsány.



Obrázek 7 – software GetDataBack for NTFS „vlastní tvorba“

4.6 Experiment

V roce 2002 provedli studenti Simson Garfinkel a Abhi Shelat z MIT (Massachusetts Institute of Technology) zajímavý experiment. Ten spočíval v tom, že za méně než 1000 dolarů pořídili 158 použitých pevných disků, z nichž 129 bylo funkčních. Disky koupili převážně přes eBay, aby tak zajistili co největší geografické pokrytí. Následně z nich získali nesmazaná data a ta smazaná se pokusili obnovit. Cíl byl jediný – otestovat, kolik citlivých informací lze touto cestou získat od neopatrných uživatelů výpočetní techniky. Ačkoliv se nejednalo o výzkum příliš velkého rozsahu, výsledek byl natolik šokující, že byl ***publikován v IEEE Security and Privacy 2003****:*

U 28 disků se předchozí majitelé ani nepokusili svá osobní data smazat.

Jeden z disků obsahoval data o finančních transakcích provedených v průběhu jednoho roku, tento disk totiž pocházel z bankomatu.

Pokusy o smazání dat původními uživateli byly spíše úsměvné, neboť k tomu použili pouze standardní mazání, které poskytuje operační systém Windows.

60 procent disků bylo sice zformátováno, ale vzhledem k tomu, že příkaz „format" ve Windows nepřepisuje každý blok pevného disku, na jednom z takto zformátovaných disků bylo nalezeno přes 5 000 čísel kreditních karet.

Dále se našly údaje, jako jsou detailní osobní a finanční informace, značné množství lékařských záznamů, mnoho GB dat osobní emailové komunikace a pornografie.

[7]

Na základě tohoto experimentu se autor této práce rozhodl udělat experiment v menším měřítku, ale s podobným zaměřením. Experiment byl proveden na dvou použitých pevných discích a to: „Seagate Barracuda 7200.9 80GB“ a „WD Caviar 400 40GB“. K obnově dat byl využit software GetDataBack, který v obou případech pomohl získat zpět většinu dat.

4.6.1 Disk Seagate Barracuda 7200.9

Tento disk byl získán přes inzerát na serveru http://pcbazar.kontakt.cz . Připojení přes běžné SATA rozhraní nedělalo žádné problémy. Disk se po standardním připojení choval jako prázdný disk čistě naformátovaný souborovým systémem NTFS. Po analýze programem „GetDataBack for NTFS“ byly objeveny smazané záznamy v MFT tabulce. Všechna data byla způsobilá k obnově, takže se označil kompletní strom souborů a program se nechal pracovat. Po cca jedné hodině byl celý proces hotový a mohlo se zkusit, co všechno se na disku najde. Jelikož se na disku nacházela předchozí instalace Windows, jak se později zjistilo, konkrétně Windows XP Professional SP3, byly učiněny pokusy na start kompletního systému. Pomocí série úprav BIOSu a ovladačů bylo dosaženo stavu, kdy kompletně nastartoval „smazaný“ systém. Jediný přítomný uživatelský účet nebyl ani

chráněn heslem. Disk byl opravdu plný uživatelských dat. Namátkou osobní dokumenty, rodinné fotografie nebo emailová a ICQ komunikace. Z používaného prohlížeče Mozzilla Firefox verze 3.6 bylo možno vyčíst nepřeberné množství přístupových jmen včetně hesel. Shrnuto, disk obsahoval obrovské množství potencionálně zneužitelných dat.

4.6.2 Disk WD Caviar 400

Druhý pevný disk byl získán z prakticky již vyhozeného počítače určeného k odvozu na ekologickou likvidaci REMA. Nutno dodat, že odvoz na ekologickou likvidaci určitě není žádnou zárukou bezpečné likvidace dat. Připojení přes zastaralé IDE rozhraní v sobě neslo nutnost opatřit převodník IDE » USB. Disk nejevil známky žádného souborového systému, tedy vypadal jako nenaformátovaný. Analýza programem „GetDataBack for FAT“ přinesla své výsledky a byla nalezena smazaná tabulka rozdělení disku. Podařilo se obnovit tabulku rozdělení disku a s ní i FAT tabulku. Po analýze diskového obsahu bylo nutno konstatovat, že šlo o nesystémový disk obsahující záložní data. Kromě instalačních verzí různých programů byly nalezeny i cca jedno gigabytové zálohy databáze používané jedním ze zálohovaných programů. Databáze byla identifikována jako relační databáze PostgreSQL, ale přístup do databáze byl heslovaný. Ani pomocí volně šiřitelného programu „John the Ripper“, schopného dostat se přes hesla slovníkovým útokem (útok hrubou silou), se nepodařilo získat přístup do databáze, takže samotný obsah je neznámý. Podařilo se ale zjistit, že databáze spolupracuje s restauračním softwarem a je velmi pravděpodobné, že obsahuje zákaznické údaje a namarkované účty. Pravděpodobnost prolomení přístupu do databáze by však u profesionálního kryptoanalytika byla mnohem větší. Shrnuto, přítomnost zneužitelných dat nebyla přímo dokázána.

4.7 Průzkum

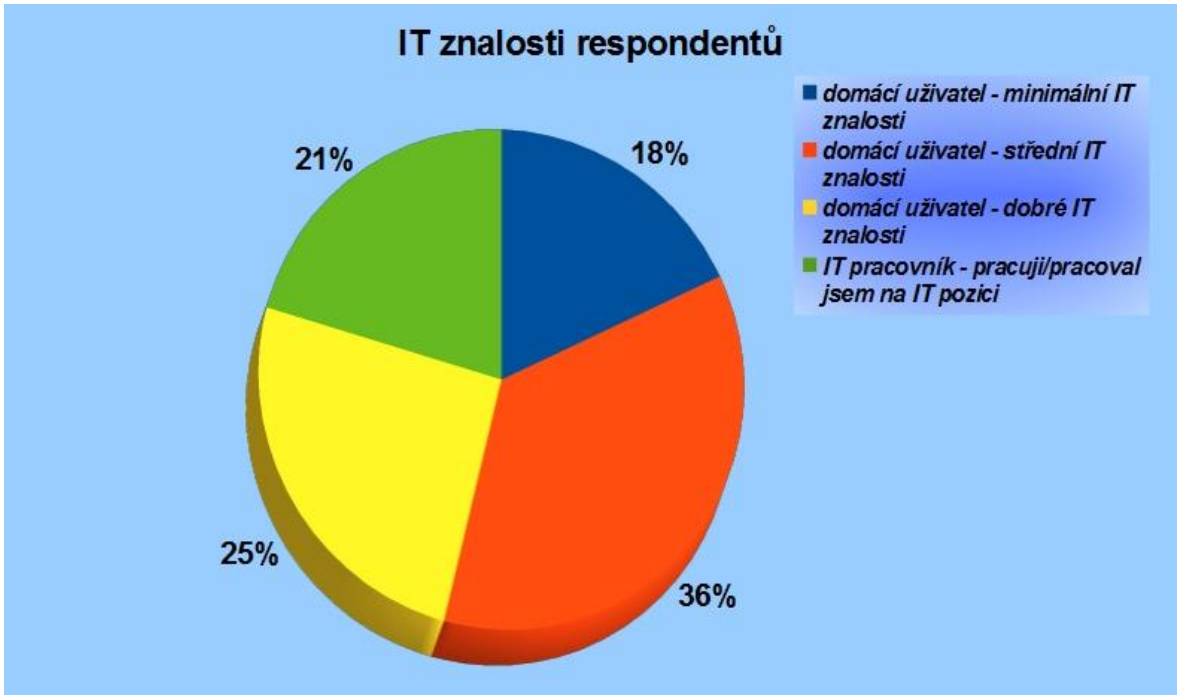
4.7.1 Nezávislý dotazník mezi 197 uživateli počítačů

Průzkum formou dotazníku byl rozšířen mezi nezávislé uživatele různými informačními kanály a zároveň byl volně přístupný po dobu jednoho týdne na stránce http://oursurvey.biz. Za toto období celý dotazník vyplnilo 197 osob. Nedokončené dotazníky nebyly zahrnuty do výsledků průzkumu. Průměrná doba strávená vyplňováním

byla změřena na 2 minuty. Skladba deseti otázek byla volena tematicky a zaměřena na obnovení dat, celkovou ochranu dat a znalosti bezpečného mazání dat.

4.7.2 Prezentované výsledky

Osoby, které vyplnily dotazník, se samy rozřadily do skupin IT znalostí podle svého úsudku a z celkových výsledků plyne, že se rozřadily vcelku realisticky. Své znalosti jako minimální označilo 18% dotázaných, jako střední 36% dotázaných, jako dobré 25% dotázaných a za IT pracovníka se označilo 21% dotázaných.

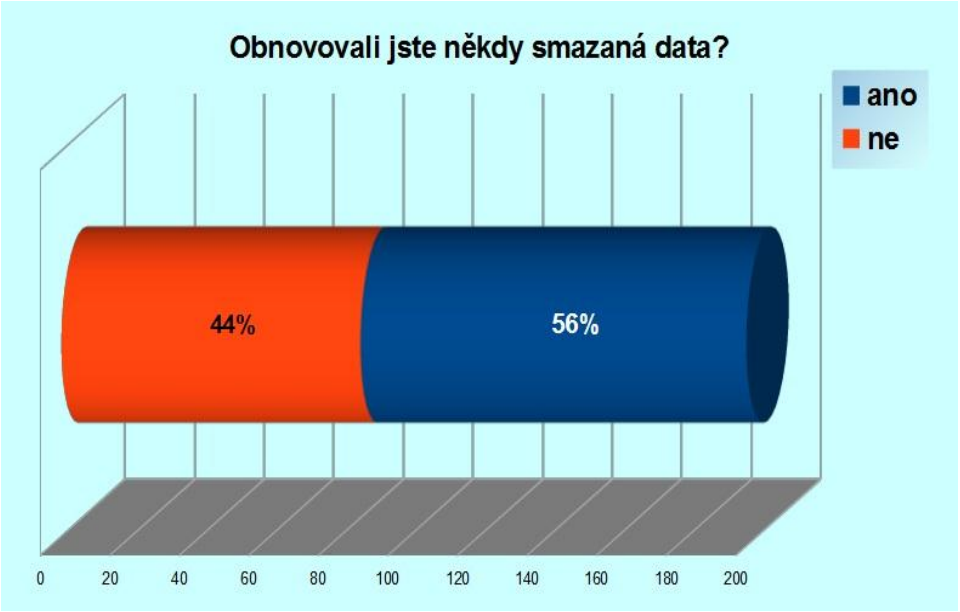


Obrázek 8 – Graf - IT znalosti respondentů „vlastní tvorba“

Svá data považuje za nenávratně ztracená v případě vyhození z koše 14% neboli 27 respondentů. Většina těchto odpovědí, konkrétně 25, pochází od respondentů, kteří označili své znalosti za nízké až střední. Na uživatele s dobrými IT znalostmi pak připadají jen 2 takovéto odpovědi a z IT pracovníků ani jeden, což se dá označit jako velice uspokojivé.

Obrázek 9 – Graf- dotazník otázka č.3 „vlastní tvorba“

Dále 65% dotázaných přiznává, že si někdy omylem smazali svá data, ale pokus o obnovení takto smazaných dat zkusilo jen 64% z nich. Celkově nějaká smazaná data obnovovalo 57% respondentů. Z pohledu IT znalostí se svá data pokusilo obnovit 15 respondentů s minimální znalostí, 31 se střední znalostí, 32 s dobrou znalostí a 35 IT pracovníků.



Obrázek 10 – Graf – obnova smazaných dat „vlastní tvorba“

Na otázku, zda respondenti přišli o svá data vinou škodlivého softwaru, odpovědělo 20% kladně, avšak nijak to nezměnilo chování této skupiny ve vztahu k zálohování svých dat. Vysoký počet dotazovaných označil, že zálohuje svá důležitá data – konktrétně 87%, což znamená, že z celé sledované skupiny nezálohuje pouhých 26 dotazovaných.

Z pohledu bezpečnosti dat a využití šifrování pro svá citlivá data odpovědělo 31% respondentů, že této možnosti aktivně využívají, 62% respondentů pak této možnosti nevyužívá a 7% respondentů netuší, co je to šifrování dat.

Je alarmující, že ač většina uživatelů ví, že vyhození z koše není definitivním krokem, tak téměř polovina z nich, přesně 46%, netuší, jak se svých dat bezpečně zbavit. Z celkového počtu odpovědí to neví dokonce 54% dotázaných. Z jednoduchých odpovědí, jak nenávratně zlikvidovat svá data, vyplynulo, že jedna polovina uživatelů volí softwarovou cestu přepisem dat a druhá polovina má blíže k destruktivním metodám.

Naopak pro autora není s podivem, že většina dotazovaných nezná svůj souborový systém. Ač 49% dotázaných odpovědělo, že svůj souborový systém znají, tak vyhodnocením odpovědí, jaký souborový systém konkrétně využívají, se zjistilo, že 24% z nich uvedlo místo souborového systému svůj operační systém. Tyto odpovědi byly tedy připočítány k odpovědím ostatních, kteří svůj souborový systém neznají. Finální verdikt tedy zní, že svůj souborový systém nezná 63% dotazovaných. Vyjádřeno procenty na každou znalostní skupinu svůj souborový systém nezná 15% respondentů označujících se za IT pracovníky, 52% respondentů s dobrými znalostmi, 64% respondentů se středními znalostmi a 71% respondentů s minimálními znalostmi.

Vyhodnocením se dále zjistilo, že věk nehraje ve znalostech dotazované skupiny významnou roli. Pro lepší statistické zpracovaní však byli respondenti rozděleni do několika věkových skupin. Zde se ukázalo silně nerovnoměrné rozdělení těchto skupin, kdy skupina mezi dvaceti a třiceti lety zabírá celých 58% ze všech respondentů. Tento jev je zřejmě dán převážně rozdělením kontaktů autora této práce a s tím i souvisejícím typickým věkem IT pracovníků.

Obrázek 11 – Graf – věkové rozdělení „vlastní tvorba“

5 Závěr

Tato bakalářská práce se zabývala bezpečným mazáním dat, obnovou dat a technickými i softwarovými prostředky jak toho dosáhnout. Dokázaným faktem zůstává, že je třeba brát rizika ztráty dat opravdu vážně. Neopatrným mazáním, případně nakládáním s datovými médii je možné přivést buď sebe anebo celý podnik do velkých problémů. Je třeba pečlivě zvážit, která data vlastně mohou být zneužitelná, a v závislosti na tom přijmout dostatečná opatření při jejich likvidaci.

Jak autor předpokládal a jak bylo průzkumem ověřeno, povědomost o metodách ničení vlastních dat je celkově nedostatečná. Lidé si svých důležitých dat začnou vážit až ve chvíli jejich ohrožení. Jak ukázal praktický experiment, lze se dostat k opravdu zajímavým a zneužitelným datům z vyhazovaných, či použitých pevných disků. Pokud by se tato data dostala do nepovolaných rukou, možné následky by byly nedozírné.

Je třeba důsledně dodržovat metody likvidace citlivých dat a nevystavovat se tak zbytečnému nebezpečí. Vhodné je též využívat šifrovací software pro zvýšení své šance na zamezení úniku dat.

Tato práce měla zohlednit všechny důležité prvky týkající se bezpečného mazání citlivých dat a autor věří, toto hledisko bylo splněno.

6 Seznam použitých zdrojů

6.1 Knižní zdroje

1. DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat, 1. Vydání: Computer Press, 2004, 190s. ISBN 80-251-0106-1

2. GOLLMANN, Dieter. Computer Security, 3. Vydání: John Willey & Sons, 2011, 434s. ISBN 978-0-470-74115-3

3. PROBST, W.,Christian a kol.. Insider Threats in Cyber Security, 1. Vydání: Springer, 2010, 247s. ISBN 978-1-4419-7132-6

4. VACCA, R., John. Computer and Information Security Handbook, 1. Vydání: Elsevier, 2009, 928s. ISBN 978-0-12-374354-1

5. BISHOP, Matt. Computer Security: Art and Science, 1. Vydání: Addison Wesley, 2003, 1136s. ISBN 0-201-44099-7

6.2 Internetové zdroje

6. Wikipedie: Otevřená encyklopedie: NTFS [online]. c2011 [citováno 29. 02. 2012]. Dostupný z WWW: <http://cs.wikipedia.org/w/index.php?title=NTFS&oldid=7811912>

7. SVOJANOVSKÝ, Petr. Nepodceňujte skartaci dat. Security World: magazín o bezpečnosti v kybernetickém světě. Praha: IDG Czech, 2010, roč. 2010, č. 3. ISSN 1802-4505.

8. České Republika. Zákon o ochraně osobních údajů. In: č. 101/2000 Sb. 2000, roč. 2011. Dostupné z: http://business.center.cz/business/pravo/zakony/oou/cast1h1.aspx#par4

9. České Republika. Trestní zákon. In: č. 40/2009 Sb. 2009, roč. 2010. Dostupné z: http://business.center.cz/business/pravo/zakony/trestni-zakonik/ravo/zakony/oou/cast1h1.aspx#par4

10. WRIGHT, Craig. *Overwriting Hard Drive Data*: *The Great Wiping Controversy* [online]. [cit. 2012-03-20]. Dostupné z: http://www.springerlink.com/content/408263ql11460147/

11. SSD Disky: nastal již jejich čas?. *ExtraNotebook* [online]. 2010[cit. 2012-03-20]. Dostupné z: http://extranotebook.cnews.cz/ssd-disky-nastal-jiz-jejich-cas

12. PŘIBYL, Tomáš. Bezpečné mazání dat z počítače. *Automatizace* [online]. 2004, roč. 47, č. 6 [cit. 2012-03-22]. Dostupné z: http://www.automatizace.cz/article.php?a=154

13. HINNER, Martin. *Filesystems*: *HOWTO* [online]. 0,8. 2007 [cit. 2012-03-22]. Dostupné z: http://tldp.org/HOWTO/Filesystems-HOWTO.html

7 Přílohy

příloha 01 – Dotazník na téma Bezpečné mazání dat, vytvořený pomocí stránky http://oursurvey.biz

1) Vaše znalosti práce s počítačem:

- (●) domácí uživatel - minimální IT znalosti
- ( ) domácí uživatel - střední IT znalosti
- ( ) domácí uživatel - dobré IT znalosti
- ( ) IT pracovník - pracuji/pracoval jsem na IT pozici

2) Stalo se Vám někdy, že jste omylem smazali svá data?

- (●) Ano
- ( ) Ne

3) Považujete vyhození souborů z koše za nenávratné?

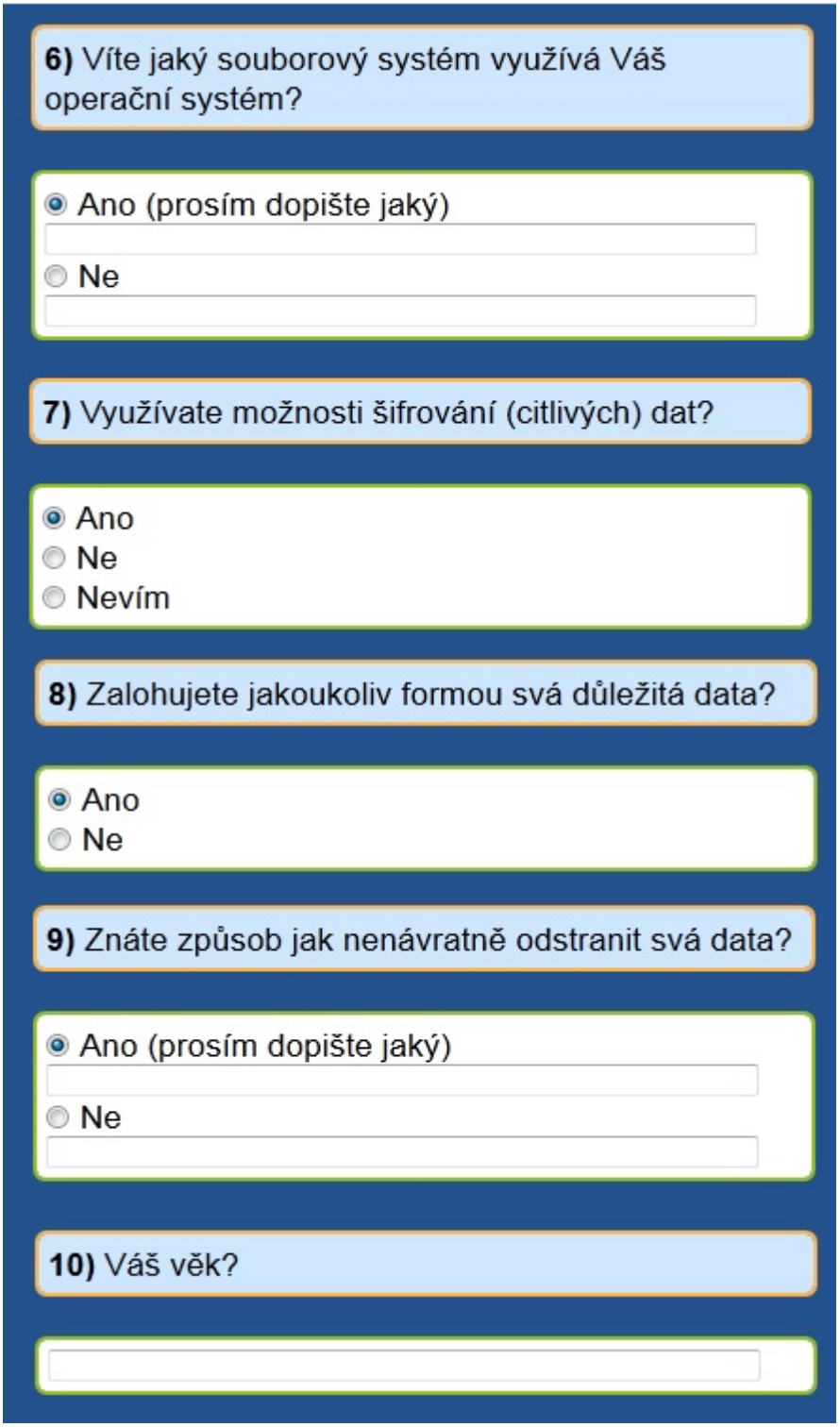
- (●) Ano (data nemohu získat zpět)
- ( ) Ne (data lze získat zpět)

4) Obnovovali jste někdy smazaná data?

- (●) Ano
- ( ) Ne

5) Přišli jste někdy o svá data vinou škodlivého softwaru? (viry, malware)

- (●) Ano
- ( ) Ne


6) Víte jaký souborový systém využívá Váš operační systém?
Ano (prosím dopište jaký)
Ne
7) Využíváte možnosti šifrování (citlivých) dat?
Ano
Ne
Nevím
8) Zalohujete jakoukoliv formou svá důležitá data?
Ano
Ne
9) Znáte způsob jak nenávratně odstranit svá data?
Ano (prosím dopište jaký)
Ne
10) Váš věk?