Digitální forenzní analýza a bezpečnost informací

Tento článek si klade za cíl přiblížit dvě základní věci – co to vlastně digitální forenzní analýza je a jak mohou být její výsledky, právě díky její specifičnosti, použity v oblasti bezpečnosti informací.

Digitální forenzní analýza (DFA) patří mezi nejmladší forenzní vědy, přestože se s ní můžeme pod různými názvy setkávat už nějakých pár desetiletí. Kolem DFA se šíří různé názory a pověsti a za svou krátkou historii už prodělala výrazný vývoj. Je tedy nezbytné některé pojmy a aplikace objasnit. Navíc má určité specifické vlastnosti, které jsou v poslední době využívány nejen pro soudní účely, ale také v oblasti bezpečnosti informací.

Co to je digitální forenzní analýza?

Na první pohled je to jednoduchá otázka, avšak opak je pravdou. Všichni sice asi intuitivně víme, o co jde, ale abychom přesněji pochopili DFA a její specifické místo v oblasti bezpečnosti, musíme si některé základní pojmy a vlastnosti vysvětlit přesněji.

DFA patří do široké skupiny forenzních věd [1]. Obecně jsou tyto vědy charakteristické tím, že se jedná o specifické (forenzní) aplikace „standardních" vědních oborů (např. soudní psychologie) nebo o samostatné forenzní disciplíny (např. daktyloskopie). DFA však z obecného pohledu nemá svoji „matku" mezi neforenzními vědeckými obory. Tím, že DFA zkoumá jakákoli digitální data [2], nelze se omezit na to, že je její neforenzní „matkou" informatika, výpočetní technika nebo zastřešující kybernetika.

Tak jako má DFA široký záběr v tom, co zkoumá, má i stejně široké možnosti uplatnění. Všude, kde se můžeme setkat s různými druhy trestního nebo jiného protiprávního jednání, můžeme se setkat také s digitálními informacemi a při odhalování použít DFA. Od porušování interních předpisů organizace, násilné trestné činnosti, podvodů, krádeží, zanedbání povinností až po hromadné ohrožení a terorismus. Dnes již digitální informace provázejí téměř každého člověka. Jejich analýzou lze získat důkazy o každém jeho kroku, činnosti.

Ne každá analýza digitálních dat však má forenzní charakter. Aby se dalo mluvit o tom, že lze výsledky analýzy použít jako důkaz (v právním smyslu slova, tedy potenciálně i u soudu), musí splňovat obecné vlastnosti forenzního zkoumání. Vyjmenujme tyto zásady, abyste mohli v základech posoudit, zda analýza, která je vydávána za forenzní, takovou skutečně je.

Legalita, tj. veškeré informace, stopy, vzorky, předměty, dokumenty atp., které slouží jako zdroj/vstup DFA, metody a způsoby zpracování, a tedy i výstupy DFA musí být získány, pořízeny a zhotoveny legálním způsobem. Případy narušení zásady *legality* jsou uvedeny v Boxu 1.

Integrita, tj. vše, co bylo prováděno, veškeré způsoby práce se vstupními informacemi (stopy, vzorky...), musí být prováděno způsobem, ze kterého je jednoznačně jasné, že nemohlo dojít k úmyslné nebo neúmyslné manipulaci nebo změně, kdo, kdy, kde, jak a proč s nimi co dělal apod. V Boxu 2 jsou uvedeny dva konkrétní příklady narušení

Případy narušení zásady Legality BOX 1

Existují podoblasti DFA, které se v současné době nazývají „Live Forensics" a „Network Forensics". Jejich jádrem je analýza dat získaných on-line, z běžících systémů (zejména z operační paměti) nebo ze síťového provozu (většinou jeho záznamem). V těchto případech se jedná o aktivní monitoring, který velice pravděpodobně může kolidovat minimálně s telekomunikačním zákonem nebo zákonem na ochranu osobních údajů. Bez právního posouzení rozsahu a účelu takového monitoringu můžeme velice lehce porušit zásadu legality.

Analýzu digitálních dat nelze provádět ručně a bez odpovídajícího programového vybavení (od operačních systémů až po speciální forenzní analytické nástroje). Je až zarážející, když znalec k dokumentaci nálezu použije screenshot okna programu, kde je zjevně vidět, že se jedná o crack.

zásady *integrity* inspirované praktickými zkušenostmi.

Opakovatelnost/přezkoumatelnost, tj. použití takových způsobů práce a jejich dokumentace tak, aby metody mohly být opakovaně provedeny stejným způsobem, čímž by se ověřilo, zda se dospěje ke stejným závěrům, nebo aby pomocí jiných ekvivalentních metod (pokud existují) mohla být správnost závěrů ověřena. V Boxu 3 jsou uvedeny další dva příklady z praxe, které ilustrují narušení zásady *opakovatelnosti/přezkoumatelnosti.*

Nepodjatost, tj. nezávislost subjektu provádějícího forenzní činnosti na zkoumaném předmětu nebo objektu.

Poznámka: Předesílám, že všechny výše uvedené atributy forenzního zkoumání nejsou podle mých informací v ČR nikde právně nebo jiným způsobem zakotveny a vycházejí pouze z best practices a ze zahraničních doporučení. Pouze *pojatost* je specifikována zákonem o znalcích a tlumočnících jako možnost, pro kterou může být znalec ze zkoumání vyloučen. Proto je vyjádření znalce k podjatosti jednou ze standardních součástí znaleckého posudku.

V Boxu 4 je uveden další příklad, kdy se nejspíše také jedná o narušení zásady *nepodjatosti*.

Neodmyslitelným atributem, který podmiňuje všechny výše uvedené, je *detailní dokumentace*. Bez ní by bylo obtížné prokázat nejen faktické závěry, ale i to, že výše uvedené atributy byly bezezbytku naplněny. Jak se to dělat nemá, ilustruje příklad nedostatečné dokumentace, viz Box 5.

Přirozeně je nutné, aby v jakékoli forenzní oblasti platil požadavek na

Příklady narušení zásady Integrity BOX 2

Úkolem jistého znalce bylo nalézt na předloženém PC veškeré dokumenty obsahující určitou specifickou informaci (jednalo se o čísla bankovních účtů). Protože znalec nebyl schopen nalézt dokumenty, které byly v době zkoumání již smazané, při revizním zkoumání jsme zjistili neuvěřitelnou věc – dotyčný „takyznalec“ na zkoumaném PC vytvořil v rootu adresář s názvem „NALEZY“. A tam překopíroval své nálezy, které posléze z toho samého počítače vytiskl přes v počítači nainstalovaný MS Word na tiskárně, kterou pro tyto účely k počítači připojil. Doufám, že k tomuto případu není potřebný žádný komentář. Kromě fatální neodbornosti zničil svým diletantstvím v oblasti zásad forenzní práce další potenciální důkazy

Jistá firma „A“ nebyla spokojena s dodávkou SW vybavení v ceně několika miliónů. Své servery s nainstalovaným systémem dala k posouzení firmě „B“. Protože však byly závěry firmy „B“ zpochybněny, došlo na přezkoumání. S údivem jsme museli konstatovat, že v zásadě sice závěry našeho předchůdce mohly odpovídat skutečnosti, avšak tento (asi ve snaze efektivně využít vše, co ve firmě je) v době mezi skončením svého posuzování a vrácením serverů zpět firmě „A“, operativně využil zkoumané servery pro vlastní potřebu – zřídil si z nich na dobu cca dvou měsíců backupovací servery. Dohra takového „takykvalifikovaného“ posuzování nebyla příjemná.

Příklady narušení zásady Opakovatelnosti /přezkoumatelnosti BOX 3

Úkolem jistého znalce bylo posouzení, zda digitální videozáznamy na dvou CD, které měly být pořízeny z jednoho zdroje s jistým časovým odstupem, jsou stejné, a tedy zda nedošlo k jejich manipulaci. Znalec použil metodu, kterou popsal jako „postupné prohlížení obou záznamů na monitoru s vysokým rozlišením, aby bylo možné rozpoznat co nejvíce detailů jednotlivých záznamů“. Tady znalec jednoznačně použil nejenom metodu nevhodnou z odborného hlediska, ale i metodu, která je díky jeho subjektivitě neopakovatelná třetí stranou.

Ještě horší situace nastala (a to je jeden z nejčastěji se vyskytujících neduhů), když znalec uvedl (cituji) „po náročném a detailním zkoumání jsem učinil závěr, že zkoumaný program někdy také špatně vkládá data do účetního modulu“, aniž by zdokumentoval, v jakých případech a jak dospěl k závěru, že data byla do účetního modulu vložena špatně. Bez popsání podmínek a postupu zkoumání není možné tento opakovat a ověřit správnost tvrzení.

Příklad pravděpodobného narušení zásady Nepodjatosti BOX 4

Znalec ve vyjádření k nezávislosti na zkoumaném objektu a subjektu píše, že sice instaloval posuzovaný systém u klienta, avšak toto bylo prováděno na základě smlouvy o dílo a zpracování znaleckého posudku na tento systém se řídí trestním řádem, tudíž se jedná o úplně jiný právní vztah. Podjatost je tedy z jeho strany vyloučena.

Příklad nedostatečné dokumentace BOX 5

Znalec byl pověřen zkoumáním 22 ks CD. Jako jedinou dokumentaci toho, co zkoumal, použil fotografii zavřené krabičky na CD (spindl pro 50 ks CD), ve které se daly tušit nějaké CD nosiče. S odstupem více než jednoho roku bylo nutné revizní zkoumání těchto nosičů. I když se jednalo o relativně triviální problematiku, hned v úvodu jsme byli nuceni konstatovat, že z důvodu špatně provedené dokumentace předchozího posudku nemůžeme zaručit, že CD, která byla předložena k reviznímu zkoumání, jsou stejná jako předmět zkoumání posudku původního. Důsledky byly značné a došlo až na zpochybnění celého předchozího důkazního řízení.

odbornost. Zdá se to být samozřejmé, ale jsou určité obory (a zkoumání digitálních dat z důvodu extrémní dynamiky vývoje k nim jednoznačně patří), kde musí být odbornost neustále doplňována a (měla by být) neustále ověřována. Výše uvedené příklady z praxe to jen potvrzují.

Závěrem této části snad jen jedna typická negativní charakteristika znaleckých závěrů, která nemá nic společného s forenzními zásadami. Část našich znalců (alespoň podle toho, co jsme měli možnost zjistit při zpracování revizních posudků) pravděpodobně neví, že je zásadní rozdíl mezi tím, co by chtěli (kulantně řečeno mezi jejich odborným názorem), a tím, co je možné jednoznačně dokázat. Forenzní analýza, DFA nevyjímaje, je totiž o důkazech, ne o odborných názorech nebo pocitech.

Digitální forenzní analýza a bezpečnost informací

DFA má nezastupitelné místo v systému reakcí na bezpečnostní incidenty (Incident Response Handling – IRH). Již od prvního vydání normy ISO/IEC TR 18 044 v roce 2004 je DFA věnována pozornost v celkovém systému IRH. Obdobně tomu je i v ISO/IEC 27002, kde přibyla samostatná kapitola o IRH, v jejímž rámci má sběr a vyhodnocení důkazů (jinak digitální forenzní analýza) své místo. Tím se DFA oficiálně dostává z oblasti specificky soudních aplikací do základních požadavků na ochranu bezpečnosti informací obecně jako součást preventivních bezpečnostních opatření.

Přestože obě výše zmíněné normy nejsou normami specificky technologickými, rád bych podtrhl přístup k IRH jako obecný, jako reakci na incidenty obecné povahy, nejen na IT/IS incidenty. K řešení incidentů v organizacích musíme tedy vždy přistupovat ve dvou základních rovinách úzce spolu souvisejících:

- *První rovina je „funkční“* a je v zásadě popsána ve výše zmíněných normách, kde je základním cílem systému IRH (kromě připravenosti) incident včas identifikovat a analyzovat, zamezit jeho šíření, obnovit funkčnost po incidentu a poučit se z něj, aby se neopakoval.

- *Druhá rovina je „finanční“* a v normách není explicitně pojmenována, protože nemá přímou souvislost s IT/IS. Jedná se o to, že jakýkoli incident má dopad na organizaci nejen z hlediska funkčnosti, ale způsobuje přímé a nepřímé materiální ztráty.

Úlohu DFA v obou pohledech na IRH ilustruje další příklad z praxe, viz Box 6.

Příklad použití DFA v procesu IRH — BOX 6

Společnost provozovala webový portál, jehož prostřednictvím poskytovala část služeb svým klientům. Po prvním upozornění od providera, že je jejich server zdrojem útoků na jiné internetové servery, společnost server přeinstalovala, avšak po 14 dnech přišlo další upozornění, že se útoky opět opakují. Naším úkolem bylo zjistit tři základní věci:

1. Jak a proč bylo možné, že byl jejich server hacknutý, a kde se stala v konfiguraci resp. zabezpečení chyba, která to umožnila.
2. Identifikovat zdroj útoku na jejich server tak, aby bylo možné podat trestné oznámení na pachatele tohoto útoku.
3. Identifikovat veškeré systémy, procesy a činnosti společnosti, které byly útokem dotčeny.

V první části nebylo řešení až tak složité a po identifikaci programu, který útoky způsoboval, a technickém auditu bezpečnostní konfigurace serveru byla v relativně krátké době několika málo hodin nalezena příčina i způsob odstranění problému a společnost mohla opětovně bezpečně zprovoznit server.

V druhé části, která již nebyla tak jednoduchá, nám pomohlo, že provozovatel, aniž by to dle svého vyjádření dělal cíleně, logoval spíše omylem velké množství různých informací o běhu systému, a také neopatrnost útočníka, který za sebou nemazal stopy. Nakonec nám pomohlo i trochu štěstí, protože útočník byl identifikován v ČR a měli jsme tak k jeho potvrzení mnohem více dostupných nezávislých informačních zdrojů. Společnost tak získala dostatek důkazů k tomu, aby mohla podat trestní oznámení a pokusit se vymoci škodu, která jí byla způsobena.

Třetí část analýzy byla splněna pouze částečně, protože v rámci našich kompetencí jsme nemohli stanovit některé procesy činnosti nemající přímou souvislost s rozsahem našeho znaleckého oprávnění. Nicméně naše nálezy posloužily jako hodnotné vstupy pro vyčíslení škody, která byla společnosti útokem způsobena.

Jsem přesvědčen, že v podobných situacích jsou i u vás prováděny obdobné činnosti (minimálně v rozsahu první části popsaného příkladu), avšak zřídka způsobem, který splňuje veškeré atributy forenzní analýzy uvedené výše. Důkazní síla takových ryze technických analýz je výrazně nižší a navíc v případě, že by došlo i na soudní spor a vymáhání škody, běžné neforenzní postupy by neměly velkou šanci v soudním sporu obstát. To je pravděpodobně i hlavní příčina toho, že „finanční rovina“ řešení incidentů má v našich podmínkách malou šanci na úspěch a škody i běžných incidentů se nevyčíslují a následně ani nevymáhají na původcích incidentů, naopak zbytečně zvyšují interní náklady organizace (a v případě IT/IS incidentů náklady útvarů IT) a narušují jejich už tak napjaté rozpočty.

Je potřeba ještě jednou zdůraznit, že DFA může přinést důkazy o téměř jakémkoli incidentu v organizaci (nejen in-

cidentu v IT/IS) a výrazným způsobem posílit výsledky „obecných“ interních šetření nebo auditů, které dnes a denně v organizacích při jakýchkoli incidentech probíhají.

Začlenění DFA do celkového řídicího systému organizace (ať už do procesů ISMS nebo procesů interních auditů) je v současnosti označováno pojmem „forensic readiness“[3]. Účelem implementace „forensic readiness“ je zejména:

- poskytnout organizaci nástroje a možnosti k tomu, aby mohla důsledně došetřit veškeré incidenty (způsobem popsaným v uvedeném příkladě);
- naučit ji získávat důkazy, umožnit jí vymáhat vzniklé škody a velmi výrazně tím zvýšit její šance na úspěch v případných právních sporech;
- zajistit, aby v případech (zejména velkých majetkových) problémů měly kontrolní a vyšetřovací orgány k dispozici informace, které mají váhu důkazů. Tyto požadavky vznikly zejména v USA jako reakce na značné problémy, které komplikovaly řešení případu Enron a dalších navazujících kauz (USA – Federal Rules of Civil Procedure, 2006) a byly ještě více eskalovány dalšími problémy souvisejícími s aktuální celosvětovou hospodářskou krizí.

„Forensic readiness“ tak umožňuje nejen získávání důkazů v procesu IRH, ale také nastavení interních mechanizmů tak, aby s veškerými důležitými informacemi o chodu organizace bylo nakládáno způsobem, který zaručí jejich důkazní sílu.

Jedním ze způsobů, jak implementovat požadavky „forensic readiness“ v organizaci, je použití systémů typu e-Discovery[4]. Jedná se o komplex personálních, organizačních a technických opatření, které umožňují v zásadě komplexní přehled o všech informacích, které se v organizaci nacházejí, a navíc způsobem, který odpovídá zásadám forenzní práce.

Zjednodušeně lze říci, že se jedná o nasazení softwarových agentů na všechny komponenty IS tak, aby v případě incidentu bylo umožněno efektivní provedení DFA on-line kdekoli a kdykoli v rámci organizace. Navíc jsou takové systémy schopné nejen ex-post analyzovat děje a procesy v informačních systémech, ale i proaktivně monitorovat např. citlivé informace organizace a jejich šíření, aktivně zasahovat do systémů v případě akutního incidentu apod. Nedílnou součástí takto citlivých systémů je ošetření rolí, pravomocí, přístupových práv a detailní logování veškerých aktivit, které jsou systémem prováděny. Samozřejmostí je dodržení všech výše uvedených zásad forenzní práce.

Závěr

Nebývá v našich podmínkách obvyklé plně implementovat všechna (někdy možná až schizofrenická) pravidla, která k nám přicházejí zejména z USA. Z druhé strany je potřeba zdůraznit, že v případě e-Discovery se jedná o unikátní řešení, která jsou při rozumné implementaci (a musím zdůraznit, že také při dodržení veškerých právních norem) schopna vyřešit velké množství problémů, se kterými se setkáváme právě při implementacích IRH systémů. Ukazují nám také tendence, kudy se bezpochyby v blízké budoucnosti bude ubírat celkové chápání ochrany klíčových informací u nás. Až se tu povede nastavit rozumnou rovnováhu mezi ochranou soukromí jednotlivce a ochranou podnikatelských cílů, DFA se stane jedním z nejdůležitějších bezpečnostních opatření.

Při potenciální implementaci e-Discovery systémů musíme mít vždy na mysli, že jejich původ pochází z metod DFA. Tyto metody vynikají (právě díky svým základním charakteristikám, které byly popsány v první části článku) vysokou mírou transparentnosti a jejich použití by mělo být zárukou, že nebudou porušeny žádné další zákonem chráněné zájmy. Jak však dokreslují příklady z praxe, do ideálního stavu ještě máme co dohánět.

Marián Svetlík
svetlik@rac.cz

Ing. Marián Svetlík

Od ukončení vysokoškolského studia v roce 1983 pracoval v různých oblastech IT/IS. Od roku 2000 je vedoucím konzultantem a vedoucím znaleckého ústavu digitálních forenzních analýz společnosti Risk Analysis Consultants, s.r.o..

POUŽITÁ LITERATURA

[1] *Forensic Science*, http://en.wikipedia.org/wiki/Forensic_science
[2] *Computer Forensics*, http://en.wikipedia.org/wiki/Digital_forensics
[3] ROWLINGSON, R. *A Ten Steps Process for Forensic Readiness. International Journal of Digital Evidence*, Winter 2004, Volume 2, Issue 3. http://www.utica.edu/academic/institutes/ecii/publications/articles/A0B13342-B4E0-1F6A-156F501C49CF5F51.pdf
[4] K&L Gates LLP. *E-Discovery Amendments to the Federal Rules of Civil Procedure Go Into Effect Today. Blog on Electronic Discovery Law*, 1. 12. 2006. http://www.ediscoverylaw.com/2006/12/articles/news-updates/ediscovery-amendments-to-the-federal-rules-of-civil-procedure-go-into-effect-today/