Eva Racková

Problematika digitálních stop

Anotace: Digitální stopy jsou velmi bohatým zdrojem informací. Při jejich shromažďování, analýze a uchovávání musí být dodržovány některá základní pravidla, jinak mohou být tyto stopy bezcenné.

Klíčová slova: bezpečnostní management, digitální stopa, počítačová kriminalita.

Objemy dat, produkované informačními systémy po celém světě, narůstají geometrickou řadou. Kromě dat produkovaných lidmi (např. psaní textů nebo zadávání dat do databáze) vznikají velké objemy dalších dat, které jsou generovány přímo informačními systémy. Oba typy dat však mají jedno společné: jsou velmi zajímavým zdrojem informací o všech oblastech lidské činnosti. Ačkoliv jsou digitální stopy využívány a dokonce cíleně hledány při vyšetřování některých typů trestných činů, není zpracování digitálních stop zatím podchyceno v celé jejich šíři a příslušné postupy nejsou součástí standardních postupů vyšetřovacích orgánů. Cílem tohoto příspěvku je naznačit, jaké typy digitálních stop běžně vznikají a jaká pravidla je třeba zachovávat při jejich zajišťování.

1 Úvod

Digitální stopy jsou dnes rutinně využívány při řešení řady trestných činů, typicky např. šíření dětské pornografie. Digitální stopy však mohou významně přispět k objasnění mnoha dalších trestných činů. Jejich využití při vyšetřování většiny trestných činů je však doposud nedostatečné. Svoji roli hrají jak nedostatek pracovníků s příslušnou specializací (zajišťování a zpracování digitálních stop), tak nedostatečná informovanost provozních pracovníků, kteří si nejsou vědomi bohatství informací, které se v informačních systémech nebo i v běžném osobním počítači skrývají a které mohou významně přispět k úspěchu vyšetřování. Cílem tohoto příspěvku je naznačit, jaké typy stop v informačních systémech vznikají a jakým způsobem je možné je využít. Vzhledem k rozsahu příspěvku jde pouze o úvod do této problematiky, který by pro praktické potřeby bylo třeba dále rozpracovat.

2 Typy shromažďovaných digitálních stop

Digitální stopy jsou v dnešním technikou nabitém světě všudypřítomné. Vznikají nejen v počítačích, ale také např. při telefonních hovorech nebo v různých digitálních přístrojích (osobní organizéry, fotoaparáty, kamery apod.). Principielně jsou tyto stopy trojího charakteru:

- člověkem záměrně vytvořené stopy, např. textové soubory, tabulky, prezentace, databáze, fotografie, zvukové nahrávky apod. Do této skupiny patří i kopie těchto stop (např. zálohy na různých typech médií) a dočasné soubory (temporary files);
- stopy, které vznikají automaticky při fungování příslušného systému nebo zařízení. Takovými stopami mohou být např.:
    - metadata, např. u textových souborů informace o autorovi, datu vytvoření, datu poslední modifikace, počtu znaků apod.;
    - záznamy o fungování systému nebo zařízení, tzv. logy. Sem patří záznamy operačního systému, jednotlivých aplikací (včetně např. internetového

prohlížeče a jím ukládaných informací), ale také aktivních síťových prvků, firewallů apod. Přehled nejběžnějších typů logů je uveden v tabulce 1[1];
    - systémové informace, tj. informace, které daný systém ukládá a využívá pro účely svého vlastního fungování (např. informace v registrech systému Windows, informace o oprávněných uživatelích systému a jejich právech, informace o přístupových právech ke konkrétnímu objektu informačního systému);
    - komunikační informace
- zbytková data, tedy data, která byla uživatelem nebo systémem odstraněna a přesto je možné je v informačním systému najít a využít. Sem patří i data, která uživatel záměrně schoval do nevyužitých částí úložného prostoru.

Vzhledem k šíři a různorodosti systémů a zařízení, která vytvářejí digitální stopy, není a nemůže být výše uvedený seznam vyčerpávající.

Tabulka 1: Nejběžnější typy logů

Typ logu	**Popis**
Záznamy o internetových aktivitách	Jednotlivé osobní počítače uchovávají záznamy o aktivitách uživatelů v několika formách. Pro přístup na internetové stránky se nejčastěji používají aplikace Internet Explorer, Firefox, Mozilla a Netscape. Např. Internet Explorer uchovává informace o aktivitách uživatele v souboru Content.IE5. Tento soubor je obvykle uložen v adresáři *Documents and Settings\<jméno uživatele>\Local Settings\Temporary Internet Files\Content.IE5*. Tento soubor obsahuje kopii internetových stránek, které si daný uživatel prohlížel. Počítač používá tyto kopie pro případ, že by si uživatel chtěl prohlédnout znovu některou ze stránek, které již viděl. Počítač ji v takovém případě nemusí znovu stahovat ze serveru a použije kopii uloženou v souboru Content.IE5. Pokud používá počítač více uživatelů a každý má své vlastní uživatelské jméno (a heslo), pak má každý uživatel také svůj vlastní soubor Content.IE5. Lze tedy rozlišit stránky, které prohlíželi jednotliví uživatelé. Výhodou souboru Content.IE5 je, že obsahuje kopie stránek ve stavu, v jakém je viděl uživatel a který se může významně lišit od aktuální verze. Dalším adresářem, který obsahuje relevantní informace, je adresář History.IE5. Tento adresář je obvykle umístěn také v Local Settings (Documents and Settings\<jmeno uzivatele>\Local Settings\History\History.IE5. Soubor History.IE5 neobsahuje kopie stránek, ale odkazy na stránky, které uživatel navštívil. Při kliknutí na odkaz se tedy dostaneme na živou internetovou stránku. Tyto odkazy jsou navíc utříděny podle období, kdy je uživatel navštívil (např. před třemi týdny, před dvěma týdny, minulý týden, v pondělí, v úterý apod.), a podle zdroje (například všechny stránky uložené lokálně na počítači a navštívené uživatelem jsou v jednom adresáři). Soubor obsahuje také informace o datu a čase, kdy byl příslušný odkaz použit, a informaci o počtu návštěv. Posledním místem, kde jsou uchovávány informace o aktivitách uživatelů na Internetu, jsou uchovávány v souborech Cookies. Cookies jsou zprávy, které web

[1] Podle Directors and Corporate Advisors Guide to Digital Investigations and Evidence, Information Assurance Advisory Council (IAAC), 2005, www.iaac.org.uk

	server zasílá webovému prohlížeči, který je ukládá v textových souborech. Tyto zprávy jsou pak zasílány zpět webovému serveru pokaždé, když ho uživatel navštíví. Webový server je schopen podle těchto zpráv identifikovat uživatele a upravit příslušnou webovou stránku podle předchozích preferencí uživatele.
Logy antivirových programů	Informační systémy jsou v naprosté většině chráněny antivirovými programy. U velkých systémů jsou antivirové programy instalovány na všech jeho komponentách. Tyto programy obvykle ukládají informace o nalezených virech a podobných škodlivých programech a způsobu jejich zneškodnění. Tyto informace je možné využít ke zjištění, zda mohl být příslušný incident způsoben škodlivými programy nebo nikoliv.
Logy operačních systémů	Většina operačních systémů umožňuje nastavit tvorbu logů jak na serverech, tak na úrovni jednotlivých pracovních stanic. Tyto logy pak poskytují řadu informací o přihlášení a odhlášení konkrétního uživatele a případně další informace o jeho aktivitách v informačním systému.
Logy databází	Většina databází umožňuje vytváření poměrně podrobných záznamů o svém fungování. Ve většině případů však jako uživatelé databáze nejsou identifikováni konkrétní uživatelé, ale aplikace, které danou databázi využívají. Databázové logy jsou pak zdrojem informací zejména o přímém přístupu (např. administrátorů nebo útočníků) do databáze, kdy neplatí bezpečnostní pravidla vynucená aplikací.
Aplikační logy	Většina aplikací umožňuje vytváření relativně podrobných záznamů o svém provozu. Tyto logy pak mohou sloužit k identifikaci konkrétních aktivit jednotlivých uživatelů a administrátorů.
Logy na telefonních ústřednách	Informace o uskutečněných hovorech slouží spíše jako podpůrné informace o komunikaci s dalšími osobami. Telefonní přístroje jsou obvykle volně přístupné a není možné uskutečněný hovor přiřadit konkrétní osobě. K dispozici je pak obvykle jen volené číslo a čas a délka volání.
Logy ze systémů kontroly přístupu	Většina organizací má poměrně dobře propracované systémy kontroly fyzického přístupu do svých prostor. Logy z elektronických systémů kontroly přístupu mohou poskytnout poměrně podrobné informace a pobytu a pohybu konkrétní osoby ve společnosti a tím podpořit informace o aktivitách této osoby získané z jiných zdrojů.

3 Využití digitálních stop

Digitální stopy je možné využít při řešení většiny druhů trestné činnosti. Tato část příspěvku naznačuje typy informací, které mohou digitální stopy obsahovat, a jejich možné využití.

3.1 Informace o aktivitách osob

Jedněmi z nejvýznamnějších digitálních stop jsou stopy obsažené v osobním počítači příslušné osoby. Osobní počítač obsahuje typicky dokumenty vytvořené majitelem počítače, které mohou vypovídat o aktivitách, zájmech nebo případných sporech majitele. Důležitou součástí analýzy vytvořených dokumentů je i analýza příslušných meta-dat, která poskytnou důležité informace o čase vytvoření konkrétního dokumentu a případně některé další údaje.

Další informace o aktivitách (profesních i zálibách) majitele poskytuje instalovaný software (účetní software, software pro architektonické návrhy nebo design, aplikace pro

zpracování hudby nebo videa, hry apod.). Řada aplikací zároveň uchovává informace o době, kdy byly konkrétním uživatelem používány. Tyto informace pak lze využít k indikaci času, který příslušná osoba trávila u počítače a aktivit, které v té době provozovala.

Osobní počítač kromě toho často obsahuje aplikace pro komunikaci s okolím: emailové programy nebo programy pro přímou komunikaci (tzv. „chat“). Tyto programy v současné době často nahrazují diář a telefonní seznam a s jejich pomocí lze identifikovat kontakty majitele počítače a často i obsah komunikace. Většina těchto programů opět obsahuje řadu informací o čase, kdy byly jednotlivé zprávy vytvářeny, odeslány, přečteny apod.

Podobné informace vznikají v případě, kdy je osobní počítač připojen do lokální nebo rozlehlé sítě.

3.2 Informace o komunikaci s dalšími osobami

Pro řadu lidí, zejména mladšího věku, je počítač jedním z hlavních komunikačních kanálů. I v případě, že na počítači, který dotyčná osoba používá, není nalezen software pro elektronickou poštu (email), může se připojovat na některý z emailových serverů prostřednictvím webového rozhraní bez využívání klasické emailové aplikace (MS Outlook, Lotus Notes apod.). Ti, kteří počítač nevlastní, mohou komunikovat např. s využitím pracovního počítače nebo počítačů v internetové kavárně. Důležité je v tomto případě zjistit (pokud možno) všechny používané emailové adresy.

Data, která ukládají tzv. poskytovatelé internetového připojení, obsahují řadu dalších informací o komunikaci, např. internetovou adresu, ze které je za vhodných okolností možné odvodit fyzickou adresu, ze které komunikace probíhala.

Kromě emailu komunikuje řada lidí pomocí programů pro rychlé zasílání zpráv (tzv. „chat“). Tyto programy umožňují jakýsi elektronický dialog mezi dvěma uživateli. Kromě vlastního obsahu uchovávají také informaci o datu a čase, kdy byla konkrétní zpráva odeslána. V adresáři pak nelezneme seznam osob, se kterými konkrétní uživatel tento způsob komunikace navázal.

3.3 Mobilní výpočetní technika

Zcela zvláštní kapitolu představuje mobilní výpočetní technika. V posledních letech významně narůstají objemy dat, ukládaných na mobilních zařízeních. Hlavním představitelem této skupiny zařízení je přenosný počítač, notebook, který už se stává poměrně běžnou součástí vybavení nejen firem, ale i domácností. Důležitá data jsou však ukládána i v telefonních přístrojích, v tzv. smart phones nebo osobních organizátorech. Všechna tato zařízení mohou poskytnout řadu kontaktů příslušné osoby (jména, telefonní čísla, e-mailové adresy), dokladů o komunikaci s nimi (záznamy o uskutečněných hovorech, uložené e-mailové zprávy) i dokumentů.

4 Principy

Pro zajišťování digitálních stop se odborná veřejnost[2] shodla na čtyřech základních principech:

Princip 1: Žádné aktivity vyšetřovatelů a expertů nesmí změnit data uchovávaná na počítačích nebo datových médiích, která mají být v budoucnu využita při soudním řízení.

---

[2] např. Information Assurance Advisory Council: Directors and Corporate Advisors‘ Guide to Digital Investigations and Evidence, www.iaac.org.uk, 2005 nebo National High-tech Crime Unit: Good Practice Guide for Computer based Electronic Evidence, Association of Chief Police Officers,

Princip 2: Ve výjimečných případech, kdy je nezbytné přistupovat k originálním datům na počítačích nebo datových médiích, osoba, která tak činí, musí být řádně proškolena a musí být schopna vysvětlit důvody takového postupu a jeho dopady.

Princip 3: Musí být zabezpečeno pořízení a zachování auditní stopy všech aktivit prováděných s digitálními stopami. Nezávislá třetí strana musí být schopna podle těchto informací celý postup zopakovat.

Princip 4: Osoba zodpovědná za vyšetřování má celkovou zodpovědnost za dodržování zákona a těchto principů.

Tyto principy mají za úkol zajistit, že bude možné soudu prokázat, že digitální stopy, které jsou prezentovány soudu jako digitální důkazy, jsou v naprosto stejném stavu jako v okamžiku jejich zajištění. Pro digitální stopy toto není triviální úloha. Informační systémy přidávají nebo mění záznamy samy o sobě, bez zásahu uživatele. Zároveň není zcela jednoduché prokázat, že prezentované výsledky opravdu vycházejí jednoznačně ze zajištěných digitálních stop. Pro zajišťování a zpracování digitálních stop byla z tohoto důvodu navržena řada postupů, které mají za úkol zajistit, že toto bude vždy možné prokázat. Principům zajišťování a zpracování digitálních stop se věnují i některé mezinárodní organizace. Mezi nejvýznamnější patří Mezinárodní organizace pro digitální důkazy (International Organization on Computer Evidence – IOCE[3]) a Internet Engineering Task Force[4].

4.1.1 Mezinárodní organizace pro digitální důkazy

V roce 1995 byla založena Mezinárodní organizace pro digitální důkazy, jejímž úkolem je vytvářet prostředí pro výměnu názorů odborníků v oblasti digitálních důkazů. Kromě toho formuluje tato organizace standardy a doporučení pro jednotlivé oblasti zajištění a využití digitálních stop. V roce 1997 se začala zabývat vývojem mezinárodních standardů pro výměnu a získávání elektronických důkazů. Za tímto účelem byly vytvořeny pracovní skupiny v Kanadě, Evropě, Velké Británii a Spojených státech. Všechny vyvíjené standardy jsou založeny na několika základních atributech:

- soulad se všemi právními systémy;
- použití běžného jazyka;
- trvalost;
- možnost fungovat bez ohledu na hranice států;
- schopnost demonstrovat důvěru v integritu důkazního materiálu;
- aplikovatelnost na všechny digitální důkazy;
- aplikovatelnost na všechny úrovně, tj. jednotlivce, organizace i stát.

Na základě těchto atributů bylo v roce 1999 přijato 5 principů:

- při zajišťování digitálního důkazního materiálu nesmí být tento materiál změněn;
- pokud je třeba využít originální důkazní materiál, může to činit pouze forenzně kompetentní osoba;
- všechny aktivity související se zajišťováním důkazního materiálu, přístupem k němu, skladováním a přenosem musí být plně dokumentovány a přezkoumatelné;

[3] www.ioce.org

[4] www.ietf.org

- konkrétní osoba je zodpovědná za všechny aktivity týkající se digitálního důkazního materiálu po dobu, kdy je tento materiál v jejich držení;
- jakákoliv organizace, která je zodpovědná za zajišťování digitálního důkazního materiálu, přístup k němu, skladování nebo přenos, je zodpovědná za dodržení těchto principů.

IOCE doporučuje k diskusi ještě další tři oblasti:
- forenzní kompetence a potřeba shodnout se na mezinárodní akreditaci a validaci nástrojů, technik a školení;
- otázky týkající se postupů pro zkoumání digitálního důkazního materiálu;
- sdílení informací, které se vztahují k hi-tech kriminalitě a forenznímu šetření;
- v informačních systémech, jako např. událostí, nástrojů a postupů, využívaných na podporu forenzního vyšetřování.

4.1.2 Internet Engineering Task Force - Request for Comment 3227

O definici požadavků na digitální stopy se pokusila i další autorita: Internet Enginnering Task Force, který vydává svá doporučení v podobě tzv. Requests for Comment (RFC). V únoru 2006 vydal Request for Comment 3227: Guidelines for Evidence Collection and Archiving (Směrnice pro shromažďování a archivaci důkazů – RFC 3227). Tato směrnice by pak měla sloužit jako podklad, na jehož základě budou vypracovány podrobné směrnice jednotlivých organizací pro tuto oblast.

Pro sběr digitálních důkazů stanoví dokument následující pravidla:
- soulad s bezpečnostní politikou organizace a zapojení vhodných specialistů v oblasti digitálních důkazů a práva;
- co nejpřesnější zachycení stavu systému;
- udržování podrobných poznámek včetně data a času. Pokud je to možné, je vhodné použít automatický transkript. Veškeré poznámky a výtisky musí být podepsány a označeny datem a časem;
- zjištění rozdílu mezi systémovým časem a UTC. U každého časového razítka by měla být poznámka, zda je použit UTC nebo místní čas;
- příprava na poskytnutí svědecké výpovědi (případně i po mnoha letech) o provedených aktivitách, včetně času, kdy byly provedeny. Podrobné poznámky budou v tom případě velmi důležité;
- minimalizace změn dat při jejich zajištění. To se netýká pouze změn obsahu, ale také např. časů přístupu k souborům nebo adresářům;
- zamezení zásahů zvenčí;
- pokud je třeba se rozhodnout mezi sběrem a vyhodnocením dat, sběr by měl mít přednost, analýza může být provedena později;
- procedury musí být realizovatelné. Jednotlivé postupy by měly být testovány, aby bylo jisté, že jsou proveditelné, obzvláště v případě krize. Jednotlivé postupy by měly být, kde je to možné, automatizovány. Je třeba postupovat metodicky;
- pro každé zařízení by měl být přijat metodický postup, který bude v souladu s principy, zakotvenými v politice shromažďování digitálních důkazů. Rychlost je v těchto případech často kritická a je tedy často nutné rozdělit práci mezi jednotlivé specialisty, aby shromažďovali důkazy paralelně. Na jednom konkrétním zařízení by se však mělo postupovat systematicky krok za krokem;

- postupovat od volatilních[5] k méně volatilním digitálním stopám. Níže je uveden příklad pořadí volatility pro typický systém:
    - registry, vyrovnávací paměť (cache);
    - směrovací tabulky, arp cache, tabulky procesů, statistiky kernelu, paměť;
    - dočasné soubory;
    - disk;
    - relevantní data o vzdáleném přihlášení a monitorování;
    - fyzická konfigurace, síťová topologie;
    - archivní média;
- vytvoření bitové kopie jednotlivých médií. Pokud bude třeba provádět forenzní analýzu, bude třeba vytvořit bitovou kopii, protože analýza se bude téměř jistě týkat např. časů přístupu k jednotlivým souborům.

Směrnice zároveň upozorňuje na skutečnosti, které mohou vést k poškození nebo zničení digitálních důkazů (i neúmyslné), a stanoví dodatečná pravidla, jak se jim vyhnout:

- nevypínat počítač, dokud nebyl skončen sběr důkazů. Většina stop může být ztracena a útočník mohl pozměnit startovací nebo vypínací procedury nebo služby tak, aby zničily digitální stopy;
- nevěřit programům, které jsou přítomné v systému. Programy pro sběr důkazů je třeba spouštět z vhodně zabezpečených médií;
- nespouštět programy, které modifikují přístupové časy souborů v systému (např. „tar“ nebo „xcopy“);
- při uzavírání externích přístupů si být vědom toho, že i tato aktivita může aktivovat mechanismy, které zničí digitální stopy.

Směrnice stanoví i postup pro shromažďování digitálních důkazů:

- identifikace toho, kde jsou digitální stopy, vypracování seznamu systémů, kterých se incident týkal a ze kterých mohou být získány digitální stopy;
- stanovení toho, které stopy jsou relevantní a přípustné, v případech nejistoty se doporučuje zajistit více stop;
- stanovit pořadí volatility pro každý systém;
- odstranit externí přístupy;
- zajistit stopy podle pořadí volatility;
- zdokumentovat posun systémového času;
- opakovaně v průběhu zajišťování stop zvažovat další možné zdroje stop;
- zdokumentovat každý krok;
- zdokumentovat přítomnost a chování osob.

Kromě toho stanoví směrnice požadavky na digitální důkazy, pokud mají být právně akceptovatelné. Digitální důkazy musí být:

- přípustné: tj. musí být v souladu s požadavky právních norem;
- autentické: tj. musí být možné prokázat vazbu mezi důkazním materiálem a příslušným skutkem;
- úplné: tj. nesmí se zabývat pouze vybraným aspektem příslušného skutku;
- spolehlivé: tj. žádný z kroků provedených v rámci zajišťování a zpracování důkazního materiálu nesmí zpochybňovat jeho autentičnost a věrohodnost;

[5] Za volatilní považujeme digitální stopy, které se při chodu informačního systému nebo zařízení mění, nejsou stálé

- věrohodné: tj. digitální důkazy musí být věrohodné a srozumitelné soudu.

Jednoznačným požadavkem je požadavek na kvalitní opatření k zabezpečení zajištěných stop. Dokumentace musí zachycovat alespoň následující atributy:

- kde, kdy a kým byly stopy objeveny a zajištěny;
- kde, kdy a kým byly stopy zpracovány nebo zkoumány;
- kdo stopy v kterých časových obdobích opatroval a jak byly uloženy;
- kdy byly stopy předány a jakým způsobem.

5 Zajišťování digitálních stop

Další text je zaměřen pouze na úvodní část procesu zpracování digitálních stop, tedy na jejich správné zajištění, které neohrozí jejich budoucí využití jak v rámci vyšetřování, tak v průběhu soudního řízení.

Při zajišťování digitálních stop je třeba dodržovat jistá pravidla, která zajistí, že zajištěné stopy budou využitelné nejen v průběhu vyšetřování, ale i jako soudní důkazy (viz principy uvedené v části 4). V každém případě platí, že tam, kde je to možné, je vhodné požádat o pomoc odborníka na digitální stopy, který je schopen zajistit digitální stopy v souladu s nejlepší praxí oboru. Pokud to možné není, je třeba dodržovat alespoň několik základních pravidel, která jsou uvedena níže.

5.1 Výpočetní technika a komunikační služby

Prvním krokem je shromáždění informací o pokud možno veškeré výpočetní technice, kterou příslušná osoba nebo osoby využívaly. Sem patří zejména osobní počítače, a to jak v domácnosti, tak na pracovišti. Je vhodné zjistit, jestli konkrétní osoba neužívala ještě další osobní počítače (kamaráda, u manželky v práci apod.). Další kategorií jsou přenosné počítače (notebooky), a to jak vlastní, tak dalších osob, se kterými mohla příslušná osoba pracovat. Dnes už téměř každý vlastní mobilní telefon, příp. mobilní telefon kombinovaný s osobním organizátorem. Opět je vhodné zjistit, zda příslušná osoba neužívala i další mobilní telefony.

Separátní kapitolou jsou komunikační služby. Většina osob dnes využívá řadu komunikačních služeb. Spoluprací s poskytovateli těchto služeb (např. telekomunikačními operátory nebo poskytovateli internetového připojení) je pak možné získat řadu informací o aktivitách příslušné osoby. V této oblasti nás tedy budou zajímat zejména emailové adresy a telefonní čísla, které příslušná osoba využívá. Budeme však **zjišťovat také** účast v internetových diskusních skupinách všeho typu. Pro účely diskusí na internetu si často účastníci zvolí přezdívku, kterou pak používají pro všechna diskusní fóra, kterých se účastní. Zjistíme-li tuto přezdívku, je možné vyhledat i další aktivity příslušné osoby.

5.2 Zajištění výpočetní techniky

Druhým krokem celého procesu je zajištění výpočetní techniky. Základním pravidlem tohoto kroku je: pokud je příslušné zařízení (počítač, telefon, notebook apod.) zapnuté, ponechte ho zapnuté; pokud je vypnuté, v žádném případě jej nezapínejte. Doporučení pro tyto dva případy jsou uvedena níže.

5.2.1 Zajištění vypnutého zařízení

Při nálezu vypnutého zařízení je třeba učinit alespoň tyto kroky:

- Zajistit místo nálezu – odchod všech osob, které se neúčastní zajištění digitálních stop.
- Nechat dokončit tisky (pokud probíhají).

- Pořídit fotografickou, případně videodokumentaci místa nálezu, včetně detailů zapojení jednotlivých zařízení.
- Ohledat místo nálezu a společně se zařízením zajistit také předměty, které se nalézají v jeho blízkosti (např. manuály, výtisky a poznámky, včetně poznámek odhozených do odpadkového koše) a periferní zařízení (tiskárna, kabely, scannery apod.). Jednotlivé předměty zajistit, označit a zdokumentovat, včetně výrobních čísel jednotlivých zařízení.
- Pokusit se zjistit přístupová hesla (např. dotazem příslušné osoby), a pokud jsou získána, zdokumentovat je.
- Podrobně dokumentovat všechny výše popsané kroky.

5.2.2 Zajištění zapnutého zařízení

Zapnutá zařízení obsahují část potenciálně cenných informací v paměti, která se vymaže při vypnutí přístroje. Proto je vhodné zajistit digitální stopy z této paměti přímo na místě před vypnutím přístroje. Kromě kroků uvedených v kapitole 5.2.1 je třeba učinit některé další kroky, které umožní zajistit maximum dostupných digitálních stop. Postupy užívané pro zajištění těchto digitálních stop však překračují rozsah tohoto příspěvku.

6 Kvalita stopy a její přijatelnost/využitelnost jako důkaz

Pokud mají být digitální stopy využity jako důkazní materiál, musí splňovat několik základních podmínek[6]:

- přijatelnost
- kvalita
- nepřerušitelnost důkazního řetězce.

Přijatelnost důkazního materiálu je dána trestním řádem a je mimo rozsah tohoto příspěvku. Další text se tedy věnuje zejména otázce kvality digitálních stop a nepřerušitelnosti důkazního řetězce.

6.1 Kvalita digitální stopy

Kvalita digitální stopy je vlastnost, kterou nelze z vědeckého hlediska objektivně měřit. Je tedy třeba najít jiný způsob, jak kvalitu posuzovat. Jednou z možností je stanovit sadu požadavků na vlastnosti digitální stopy a hledat vodítka, která indikují míru naplnění těchto požadavků. Mezi takové požadované vlastnosti mohou patřit např. následující:

- autentičnost
- přesnost – tzn. že nejsou pochybnosti o kvalitě postupů použitých k zajištění stopy, její analýze a případné prezentaci soudu. Je důležité, aby bylo možné v každém okamžiku prokázat, že stopa byla zajištěna a analyzována někým, kdo je schopen celý proces podrobně popsat. Použité forenzní metody musí být transparentní, tzn. nezávislý expert musí být schopen na základě popsaného postupu ze stejného výchozího materiálu dojít ke stejným závěrům;
- úplnost – v rámci svého předmětu podává digitální stopa úplnou informaci o konkrétní události nebo okolnostech.

[6] Directors and Corporate Advisor's Guide to Digital Investigations and Evidence

Ačkoliv není objektivní měření možné, jsou obvykle okolnosti zajištění a zpracování digitální stopy popsány v posudku znalce, který musí být schopen jednotlivé aspekty popsat a před soudem obhájit.

6.2 Nepřerušitelnost důkazního řetězce

V praxi tento požadavek znamená, že je třeba soudu prokázat, že digitální stopy prezentované soudu jsou totožné s těmi, které byly zajištěny a zkoumány, a že tyto stopy nebyly nepřípustným způsobem pozměněny od okamžiku jejich vzniku do okamžiku jejich zajištění.

Z praktických důvodů je možné rozdělit celou problematiku na dvě odlišné úlohy:

- zajištění toho, že digitální stopa nebyla změněna od okamžiku vzniku do okamžiku jejího zajištění;
- zajištění toho, že digitální stopy nebyly změněny od okamžiku jejich zajištění do okamžiku jejich využití v rámci vyšetřování, případně do okamžiku jejich využití v rámci soudního řízení.

6.2.1 Od okamžiku zajištění do okamžiku jejich využití

Nezměněnost digitální stopy od okamžiku jejího vzniku do okamžiku jejího zajištění není vzhledem k charakteru stopy možná. Možné je pouze odhadnout, s jakou pravděpodobností nedošlo ke změně této stopy. Tuto pravděpodobnost pak určuje řada aspektů kontrolního prostředí, ve kterém informační systém funguje, např. přidělování přístupových práv, kvalita hesel a kontroly přístupu k informačnímu systému a pod. Posouzením souboru kontrol, které jsou uplatňovány pro přístup a využití zdrojů informačního systému, je možné zároveň určit, s jakou pravděpodobností nedošlo k pozměnění digitálních stop od okamžiku jejich vzniku. Pro kvantitativní určení této pravděpodobnosti byly navrženy různé stupnice, které se opírají o stanovení jednotlivých aspektů kontrolního prostředí. Příkladem takové stupnice je ta, uvedená v tabulce 1.l

Tabulka 1: Navrhovaná klasifikace spolehlivosti digitálních stop

Úroveň spolehlivosti	**Popis indikátoru**	**Odpovídající zhodnocení**	**Příklady**
C0	Důkazy odporují známým skutečnostem.	Chybné/nesprávné	Šetřením byly nalezeny slabiny v Internet Exploreru, které mohly umožnit pomocí skriptů vytvořit na konkrétní webové stránce podezřelé soubory, odkazy nebo oblíbené stránky. Podezřelý nevytvořil tyto položky v systému vědomě nebo úmyslně.
C1	Důkazy jsou vysoce sporné.	Vysoce nejisté	Chybějící záznamy v souborech záznamů („log files“) nebo jsou přítomny známky manipulace s těmito soubory.

C2	Je k dispozici pouze jeden zdroj důkazu, který není chráněn proti manipulaci.	Nejistý	Hlavičky emailů, „sulog“ záznamy a „syslog“ bez dalších podpůrných důkazů.
C3	Zdroj nebo zdroje důkazů jsou lépe chráněny proti manipulaci, ale neexistuje dostatek důkazů k vytvoření jednoznačného závěru nebo existují nevyjasněné rozpory mezi dostupnými důkazy.	Možný	Útok přišel z Polska, což naznačuje, že útočník mohl být z této země. Pozdější připojení však přišlo z Jižní Koreje, což naznačuje, že útočník může být někde jinde, nebo že jde o více útočníků.
C4	(a) Důkazy jsou chráněny proti manipulaci nebo (b) důkazy nejsou chráněny proti manipulaci, ale je jich více a důkazy z nezávislých zdrojů jsou v souladu.	Pravděpodobný	Poškození webové stránky mělo svůj původ v konkrétním objektu, protože „tcpwrapper“ záznamy ukazují FTP připojení z tohoto objektu v příslušném čase a záznamy přístupu na web ukazují, že stránka byla navštívena z objektu krátce po poškození.
C5	Soulad důkazů z více zdrojů, které jsou chráněné proti manipulaci. Existují však drobné nejistoty (např. časová chyba nebo ztráta dat).	Téměř jistý	IP adresa, uživatelský účet a ANI informace vede k objektu podezřelého. Monitorování internetového provozu ukazuje, že kriminální aktivity pocházejí z tohoto objektu.
C6	Důkaz je nemanipulovatelný a nezpochybnitelný.	Jistý	Ačkoliv je to zatím nepředstavitelné, podobné zdroje důkazů mohou v budoucnu existovat.

6.2.2 Od okamžiku zajištění do okamžiku využití

K zajištění nepřerušitelnosti důkazního řetězce od okamžiku zajištění digitální stopy do okamžiku jejího využití slouží dvě hlavní metody:

1. dokumentace
2. použití kontrolních součtů

Hlavní metodou pro prokázání nepřerušitelnosti důkazního řetězce od okamžiku zajištění digitálních stop je podrobná dokumentace všech kroků, které jsou v rámci zajištění a zpracování stop činěny. Jde o kombinaci označování zajištěných předmětů, popisování zjištěného stavu, fotodokumentaci a případně další metody dokumentace. Vzhledem ke

značné volatilitě digitálních dat patří ke standardním postupům pořízení digitálních součtů (v současné době obvykle za použití algoritmu MD5[7]) pořízených datových souborů.

7 Využití poznatků o digitálních stopách v praxi bezpečnostních manažerů

7.1 Definice bezpečnostního počítačového incidentu

Bezpečnostní počítačový incident je situace, kdy je nelegálním způsobem změněna dostupnost, integrita nebo důvěrnost informací organizace nebo osoby, případně takové změny hrozí. Počítačovým incidentem je i situace, kdy jsou data nebo informační systémy použity nebo používány bez svolení majitele.

Kromě této definice lze za počítačový bezpečnostní incident považovat jakoukoliv skutečnou nebo potenciální nepříznivou událost ve vztahu k bezpečnosti počítačového systému nebo počítačové sítě, případně akt porušení explicitních nebo předpokládaných bezpečnostních politik.

Na těchto definicích je důležité, že bezpečnostním počítačovým incidentem nerozumíme pouze porušení explicitních bezpečnostních pravidel, ale že sem patří i ohrožení dostupnosti informačního systému a v něm uložených informací a také jakékoliv narušení integrity těchto informací. V tomto smyslu budeme bezpečnostní počítačové incidenty chápat v celé této kapitole.

7.2 Reakce na počítačové incidenty

Řada organizací i jednotlivců je v dnešní době silně závislá na informačních systémech a jejich nepřetržitém fungování (alespoň v jistých časových úsecích, např. v pracovní době). Každý bezpečnostní incident, který ohrozí fungování informačního systému, je tedy potenciálně zdrojem vysokých ztrát. Bezpečnostní incidenty nelze naprosto vyloučit. Lze se však na ně připravit a tím minimalizovat ztráty, které daný bezpečnostní incident způsobí. Kritická je z tohoto pohledu rychlost, s jakou je schopna organizace bezpečnostní incident identifikovat a zareagovat na něj. Kromě toho je důležité jednotlivé incidenty analyzovat a tam, kde je to vhodné, implementovat opatření, která zabrání opakování podobného incidentu v budoucnu.

Jedním ze způsobů, jak zajistit co nejrychlejší identifikaci incidentů a nejúčinnější reakci na ně, je ustanovení specializované funkce reakce na počítačové incidenty. Tato funkce může mít podobu interních předpisů a postupů pro identifikaci, hlášení a řešení incidentů nebo dokonce podobu týmu pro reakci na bezpečnostní incidenty. Cílem této kapitoly je ukázat, jak je možné takovou funkci a tým vybudovat, jaké jsou základní komponenty tohoto systému a jak funguje před incidentem a v případě konkrétního incidentu.

7.3 Budování týmu reakce na incidenty

Budování týmu reakce na incidenty není snadným úkolem. Aby byly tyto aktivity úspěšné, je třeba učinit řadu dílčích kroků. Mezi nejdůležitější kroky patří následující:

- Získat podporu vedení organizace včetně garance financování;
- Setkat se s významnými zainteresovanými stranami, stanovit strategické cíle týmu, definovat „zákazníky“ týmu ;
- Navrhnout vizi činnosti týmu, která bude založena na diskusích, o:
  - zákaznících, kterým má tým poskytovat své služby;

[7] MD5 je algoritmus, který se používá k verifikaci integrity dat vytvořením 128-mi bitového otisku zprávy z dané zprávy libovolné délky, který je unikátní pro danou zprávu.

- misi, vizi a cílech týmu;
- službách, které bude tým poskytovat;
- oganizačním modelu, v kterém bude tým fungovat, a vztahu ke zřizovateli;
- financování aktivit týmu;
- zdrojích potřebných pro tým;

- komunikovat vizi a provozní plán týmu všem zainteresovaným stranám (zřizovateli, vedení, zákazníkům, apod.);
- získat zpětnou vazbu a upravit podle ní plán;
- vybudovat tým:
  - najmout a proškolit experty;
  - pořídit vybavení a infrastrukturu;
  - vypracovat politiky a postupy, podle kterých bude tým fungovat v každodenní činnosti a které budou zároveň podporovat dlouhodobé cíle týmu;
  - vypracovat postupy pro hlášení incidentů a zajistit, že zákazníci i zřizovatel rozumí rozsahu i obsahu poskytovaných služeb;
  - informovat o zahájení činnosti týmu;
  - vypracovat metodu hodnocení účinnosti fungování týmu a postupy průběžného zlepšování procesů týmu.

Je třeba rozlišit, které záznamy (logy) budou vytvářeny a archivovány za běžného chodu a které informace jsme schopni začít shromažďovat v případě konkrétního podezření. Toto rozdělení má dva hlavní důvody:

1. Objem vytvářených a archivovaných logů musí být přiměřený. Tvorba logů nesmí nadměrně zatěžovat systém a tím snižovat jeho výkon. Objem vytvářených logů musí být takový, aby jejich zálohování a archivace byly cenově dostupné.
2. Logy musí být za běžného provozu vytvářeny v souladu s dostupnou legislativou (v České republice zejména zákon č. 101/2000 o ochraně osobních údajů v platném znění).

Jako přípravu na bezpečnostní incident je třeba si klást např. následující otázky:

- Jak budou stopy prakticky získávány? Je k dispozici vhodný hardware a vhodné softwarové nástroje?
- Jak budou stopy uchovávány a jak bude prokázán „chain of custody“?
- Existují právní překážky zajišťování a uchovávání stop (např. zákon o ochraně osobních údajů)?
- Budou zajišťované stopy využitelné jako důkazní materiál? Za jakých podmínek?
- Kdo rozhodne o prioritách, pokud požadavky na zajištění digitálních stop do jisté míry kolidují s požadavky na co nejrychlejší obnovu provozu?
- Kdo rozhodne a podle jakých kriterií o povolání externích expertů?
- Jakou úlohu má v zajišťování digitálních stop hrát útvar IT?
- Kdo rozhodne o případném podání trestního oznámení?

8 Závěr

Objemy vznikajících digitálních stop stále a velmi rychle rostou. Pokud jich chceme využít při řešení potenciálních incidentů, je třeba se na to připravit jak z hlediska nastavení prostředí informačního systému, tak z hlediska procesů, které budou zahájeny po identifikaci incidentu.

Literatúra

CASEY, E. *Digital Evidence and Computer Crime*, 2004, Academic Press Elsevier, 2nd Edition London, UK

RAK, R. Digitální stopa I, In *Security Magazín č. 1*, 2005, Praha, str. 55 – 59, ISSN 1210-8723 RAK, R. Digitální stopa II, In *Security Magazín č. 2*, 2005, Praha, str. 34 – 39, ISSN 1210-8723 RAK, R., PORADA, V., DZURČANIN, Š. „Digitální stopy a místo trestného činu", *Zborník z medzinárodného odborného vedeckého seminára „Kriminalita – bezpečnost – identifikácia",* Vysoká škola bezpečnostného manažérstva v Košiciach, 15. 9. 2007 Košice, 430 stran, ISBN 978-80-89282-19-7, str. 203 – 221

Request for Comments 1321: The MD5 Message Digest Algorithm, Internet Engineering Task Force, 1992

Request for Comments 3227: Guidelines for Evidence Collection and Archiving, Internet Enginnering Task Force, 2006

Searching and Seizinig Computers and Obtaining Electronic Evidence in Criminal Investigations, Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice, 2002

~~2~~STRAUS, J. *Úvod do kriminalistiky*, 2004, str. 77, Aleš Čeněk

Formátované: Odrážky a číslovanie

Key words: security management, digital evidence, e-crime

Summary

The volume of data produced by information systems worldwide grows significantly. In addition to data prepared by people, large amounts of data are generated by the information systems themselves. Both types of data have at least one common feature: the represent a very interesting source of information about all sorts of activities. Although digital evidence is used and in many cases actively looked for during investigation of certain types of crimes, processing of digital evidence is not used as much as it could and the right processes to collect and process digital evidence are not a standard part of processes of investigators. The objective of this article is to identify the main types of digital evidence and suggest the basic principles that have to be followed when collecting and analyzing such evidence. The article is concluded by short analysis of the processes that are initiated after a security incident.

RNDr. Eva Racková,
ACCA, CISA
KPMG Česká republika, s.r.o.
e-mail: evarackova@kpmg.cz

Recenzent: prof. Ing. Václav Krajník, CSc.