Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Naše digitální stopa na počítači a na Internetu

Pavel Skalický

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Pavel Skalický

Informatika

Název práce

Naše digitální stopa na počítači a na Internetu

Název anglicky

Digital footprint on own computer and the Internet

Cíle práce

Hlavním cílem práce je charakterizovat jednotlivé typy digitálních stop a představit nejvýznamnější metody ochrany osobních dat. Dílčím cílem bakalářské práce je srovnání schopností a možností nástrojů k ochraně osobních dat na základě analýzy prostředí, infrastruktury, požadavků a možností navrhnout a implementovat vhodné řešení individuální ochrany dat.

Metodika

Metodika řešené problematiky bakalářské práce je založena na studiu a analýze odborných informačních zdrojů, ale také na praktických zkušenostech s jednotlivými produkty. Pomocí této metodiky je navrhnuto a implementováno vhodné řešení ochrany digitální stopy. Na základě syntézy teoretických poznatků a přínosů vlastního řešení budou formulovány závěry bakalářské práce.

Doporučený rozsah práce

30-40 stran

Klíčová slova

digitální stopa, ochrana dat, hesla, cookies

Doporučené zdroje informací

DOSEDĚL, T. Počítačová bezpečnost a ochrana dat. Brno: Computer Press. 2004. 190 str. ISBN 80-251-0106-1.

ECKERTOVÁ, L., DOČEKAL, D. Bezpečnost dětí na internetu: rádce zodpovědného rodiče. 1. vyd. Brno: Computer Press. 2013. 224 str. ISBN 978-80- 251-3804-5.

HOOG, A. Android Forensics. Waltham: Syngress Publishing. 2011. 432 str. ISBN 9781597496513.

LANGE, M. C. S., NIMSGER, K. M. Electronic evidence and discovery: What every lawyer should know now. Washington: American Bar Association. 2009. 429 pages. ISBN 9781604423822.

LARRY D., LARS D. Digital Forensics for Legal Professionals. 1ˆst edition. Waltham: Syngress Publishing. 2011. 368 pages. ISBN 9781597496438.

MATOUŠKOVÁ, M., HEJLÍK, L. Osobní údaje a jejich ochrana. 2. vydání. Praha: ASPI, Wolters Kluwer. 2008. 468 str. ISBN 978-80-7357-322-5.

PORADA, V. , RAK, R. Teorie digitálních stop a její aplikace v kriminalistice a forenzních vědách. Karlovarská právní revue 4/2006. ISSN 1801-2191.

Předběžný termín obhajoby

2015/16 LS – PEF

Vedoucí práce

Ing. Čestmír Halbich, CSc.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 28. 10. 2015

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 10. 11. 2015

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 14. 03. 2016

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Naše digitální stopa na počítači a na Internetu" 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 použitých zdrojů 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 14.3.2016 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Čestmíru Halbichovi, CSc. za jeho vedení a cenné rady při vytváření mé práce.

Naše digitální stopa na počítači a na Internetu

Souhrn

Cílem mé práce je nalezení způsobů toho, jak je uživatel schopen kontrolovat svou digitální stopu. Nalezení negativních dopadů na uživatele a jeho identitu. Veškeré testy provedu na volně dostupných nástrojích. Na začátku je seznámení s pojmem digitální stopa, různé pohledy na tyto stopy. Je zde popsán vznik digitálních stop a poté je formulována prevence proti zanechávání digitálních stop. Zmíněná jsou i rizika, která hrozí při zanechávání digitálních stop. V praktické části je proveden test nástrojů na skrývání digitálních stop, a na odhalování sledovacích nástrojů. Zjišťuje se, do jaké míry se lze chránit proti útokům. S následným doporučením určitých nástrojů.

Klíčová slova: cookies, internet, osobní informace, digitální stopa, bezpečnost, ochrana dat, hesla

Digital footprint on own computer and the Internet

Summary

The aim of my work is finding ways of how the user is able to control their digital footprint. Finding a negative impact on the user and his identity. All tests performed on the freely available tools. At the beginning of the introduction to the concept of digital track, different views on these tracks. There is described the emergence of digital tracks and then formulated a precaution against leaving digital traces. Said there are risks for when leaving digital traces. In the practical part, a test tool for hiding digital tracks, and detecting tracking tools. Getting to what extent can protect against attacks. The subsequent recommendation to certain instruments.

Keywords: cookies, internet, data protection, personal information, digital footprint, safety, password

Obsah

1 Obsah

Seznam obrázků

Seznam tabulek

Úvod

Toto téma jsem si vybral po dlouhém zvažování toho, co by mě zajímalo a co bych chtěl udělat. Tuto práci jsem zaměřil na nalezení nástroje na eliminaci zanechávání digitálních stop. Téma je to celkem rozsáhle a proto jsem se zaměřil jen na určité části. Na následujících řádcích se dozvíte informace o digitálních stopách. Naleznete zde informace o tom, jak se lze bránit zanechávání digitálních stop. Naleznete zde, i jaké jsou možnosti kontroly digitální stopy a jak zamezit zanechávání digitální stopy. Mimo jiné zde nalezte i jaké plyne nebezpečí ze zanechávání digitálních stop. V dnešní době se uživatele moc nechrání před zanecháváním digitálních stop. Práce je zaměřená na typy digitálních stop a na možnosti kontroly digitálních stop.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem práce je charakterizovat jednotlivé typy digitálních stop a představit nejvýznamnější metody ochrany osobních dat. Dílčím cílem bakalářské práce je srovnání schopností a možností nástrojů k ochraně osobních dat na základě analýzy prostředí, infrastruktury, požadavků a možností navrhnout a implementovat vhodné řešení individuální ochrany dat.

2.2 Metodika

Metodika řešené problematiky bakalářské práce je založena na studiu a analýze odborných informačních zdrojů, ale také na praktických zkušenostech s jednotlivými produkty. Pomocí této metodiky je navrhnuto a implementováno vhodné řešení ochrany digitální stopy. Na základě syntézy teoretických poznatků a přínosů vlastního řešení budou formulovány závěry bakalářské práce.

3 Teoretická východiska

3.1 Digitální stopa

Každý člověk po sobě zanechává v běžném životě mnoho stop. Ať už těch fyzických, nebo digitálních. Jednou z nejznámějších stop je stopa, kterou udělal Niel Amstrong na Měsíci. Digitální stopy jsou mnohem více než identita. Nelze je spojit s určitou identitou, s určitým bankovním kontem. Digitální stopy vznikají na základě naší interakce s mobilním telefonem, tabletem, počítačem, webem, televizí. Touto interakcí vznikají digitální data a metadata (data o datech) a ty vypovídají o tom, kdo jsme a co jsme dělali. Někteří lidé za tímto dokážou vidět skutečnou hodnotu. Vlastnictvím těchto dat se dostáváme na bitevní pole, na němž můžeme vyhrát ale i prohrát. (Fish, 2009)

3.1.1 Mobilní technologie, televize, web

V dnešní době není v moci jednotlivce vlastnit svojí digitální stopu nebo ji jakýmkoli způsobem řídit. Mobilní technologie nastolili nový řád. Díky mobilním technologiím přicházejí metadata se zasazením digitálních stop do sociálního kontextu. Oproti televizím a webům poskytují mobilní technologie úplně jiný, unikátní přínos.

Lidé co mají ve svém mobilním telefonu nainstalovaný operační systém Andrid, jsou sledováni. Jejich poloha je určována pomocí Wi-Fi sítí, mobilního signálu, popřípadě i podle GPS souřadnic. I když si uživatel myslí, že není sledován, opak je pravda. Na internetu je pak možné dokonce si najít svojí mapu polohy a pohybu na ní. Zobrazují se body, kde jsme byli. (Eckertová, 2013)

Lze si to vše představit, jako kohoutky ze kterých vytéká voda. Jeden kohoutek je televize, druhý je web a třetí je mobilní technologie. Vše co vytéká si lze představit jako vizualizace velikosti hodnoty. Voda, která plní nádrž, zobrazuje digitální data, která se o uživateli ukládají.

Data získaná ze zdroje označeného jako „poslech či vysílání“ zahrnují informace typu, jak dlouho uživatel sleduje daný program, harmonogram vysílání, oblíbené kanály a

obsah na který se díval. Dále se dá zjistit, zda sedí uživatel u přijímače, nebo ne. Zjistí se to velmi jednoduše, tím jestli přepíná kanály či nikoliv.

Data získaná z webu zastupují větší míru v pomyslném kbelíku s vodou. Z webu se dá zaznamenat doba pobytu na stránce, pozornost, o co se zajímáte, vyhledávaná slova, pravopis ale i historie prohlížení. S tímto souvisí zahlédnutý, vytvořený obsah, nákupy na internetu.

Data z mobilních technologií zahrnují tu největší míru v pomyslném kbelíku s vodou. Do těchto stop se dá počítat poloha zařízení, informace i o tom s kým jste v kontaktu, co si prohlížíte na internetu, veškeré vyhledávání. A mnoho dalšího. V dnešní době není problém pro operátory odposlouchávat SMS zprávy, ve kterých hledají klíčová slova. S hovory to je zatím trošku složitější, ale do budoucna ani to nebude problém.

3.2 Druhy digitální stop

Existují dvě větší kategorie digitálních stop, o kterých se zde zmíním. V každé kategorii jsou jiné stopy a ty si přiblížíme v každé příslušné části.

3.2.1 Aktivní digitální stopy

Aktivní digitální stopa vzniká interakcí uživatele a za jeho vědomí. Záměrně zveřejňuje informace o sobě. Vyplňuje registrační formuláře na různá fóra, a weby.

3.2.1.1 Sociální sítě a fóra

Jedná se o data, která o sobě uživatel zveřejňuje dobrovolně. Uživatel ví o tom, že společnost poskytující sociální si ukládá data o tom daném uživateli. Tyto data jim dává zcela dobrovolně. Na sociálních sítích jakmile jednou uživatel napíše nějaký příspěvek do diskuze, okomentuje fotku, označí, že se mu něco líbí, tak si společnost poskytující tyto služby ihned uloží vše a pak s těmito informacemi nakládá.

Velkým rizikem jsou fotografie na sociálních sítích. Většina společností má v podmínkách užívání, že jakmile něco nahrajete na jejich sociální sítě, tak si s tím mohou nakládat, jak chtějí v mezích zákona o osobních údajích.

I když se uživatel často snaží vystupovat anonymně na fórech, tak anonymita mu je zajištěna jen zdánlivě. Vždy se dá dohledat. A pokud se jedná o fóra, kde se musí uživatel předtím registrovat, musí tam vyplnit i svůj email. A pokud nepoužívá nějaký „fake“ účet, tak se dá dohledat velmi jednoduše.

Pokud není uživatel dosti rozumný, může poskytnout nějakému útočníkovi i osobní údaje, které by mu mohli pomoci v útoku na danou osobu.

3.2.1.2 Email, SMS, chat

Mnoho uživatelů si myslí, že když si píší SMS zprávy, tak je nikdo nevidí a neví, co si píší, ale opak je pravdo. Jde o to, že mobilní operátoři vyhledávají klíčová slova ve všech zprávách a pokud najdou něco závadného, tak to hlásí.

Uživatelé operačního systému android si mohou vybrat, jestli budou posílat SMS zprávy přes aplikaci integrovanou do systému, nebo přes aplikaci třetí strany. Pokud si vyberou aplikaci integrovanou do systému android tak to bude nejspíš aplikace Hangouts, která automaticky odesílá zprávy i na servery společnosti, které patří operační systém android.

U SMS zpráv se ukládají informace typu od koho to je a pro koho to je, čas odesláni a doručení, telefonní čísla.

Nick (uživatelské jméno) u emailu dokáže uživatele propojit se sociálními sítěmi, seznamkami, stránkami s erotickým obsahem. Stačí, pokud používá stejný nick pro více webových stránek. Jakmile si vytvoří stejný nick na email a další stránky už se dá propojit.

V poslední době je velká kauza, okolo toho, že jedna nejmenovaná firma, nechce odblokovat své mobilní zařízení americké FBI, protože majitel tohoto telefonu je podezřelý

z protizákonné činnosti. Jedná se o to, že tato firma má své telefony zašifrovány a soud po nich chce, aby vytvořili „zadní vrátka“ do těchto zařízení. Tato firma to považuje za nepřijatelný, protože by to mohlo mimo jiné poškodit dobrou pověst této firmy. Proč toto zmiňuji, protože komunikace přes chatovací aplikace je ve většině případů šifrována. A proto docela i bezpečná. Nemůže vás jen tak někdo odposlouchávat.

3.2.2 Pasivní digitální stopy

Pasivní digitální stopy vznikají za nevědomosti uživatele. Data se sbírají automaticky a uživatel o nich ani neví. Jsou to data zpracovaná senzory.

3.2.2.1 IP a MAC adresa

Mnoho uživatelů internetu netuší co to ta IP adresa vůbec je. Protože to ani nepotřebují vědět. A pokud jí potřebují vědět, tak řeknou někomu, kdo to ví a zná, aby jim poradil, popřípadě jim problém s IP adresou vyřešil on. A drtivá většina nemá ani ponětí že existuje nějaká MAC adresa.

Každé zařízení, které má v sobě síťovou kartu, tak má MAC adresu. Bez toho by to nešlo. MAC adresa je specifické identifikační adresa, která je dána sítové kartě při výrobě. MAC adresa se skládá ze 48 bitů a měla by se zapisovat, jako tři skupiny čtyř hexadecimálních čísel (např. 0123.4567.89ab), ale mnohem častěji je vidět v podobě 6 hexadecimálních čísel oddělených buď pomlčkou, nebo dvojtečkou (např. 01-23-45-67-89-ab, 01:23:45:67:89:ab). Jedná se zde o jedinečnost a jednoduchou identifikaci.

Ip adresa se používá ve dvou verzích a to ve verzi IPv4 a IPv6. IPv6 se začala používat pro nedostatek adres IPv4. IPv4 se skládá z 32 bitové adresy v rozsahu 0-255 (např. 192.168.1.20) v IPv4 jsou dvě pásma neveřejných IP adres, které se používají v soukromých sítích. IPv6 adresa je tvořena 128 bity (např. 0000:0000:0000:0000:0000:0000:0000:0001).

Jakmile se připojí uživatel na internet nebo do počítačové sítě, tak začne sítová karta komunikovat s ostatními prvky v síti a pokud je zapnutý DHCP server nemusí se uživatel o nic starat a je mu přidělena IP adresa v síti.

Při vstupu webovou stránku si stránka začne automaticky zjišťovat, z jaké IP adresy se na ní kdo připojuje, popřípadě i MAC adresu si zjistí. Změnit IP adresu je jednoduché ale změnit si MAC adresu taky jde, ale není to úplně triviální záležitost a většina uživatelů to neumí. Díky tomu že si dokáže zjistit IP adresu, může identifikovat odkud, z jakého světadílu, země, města/ vesnice k této stránce přistupuje.

3.2.2.2 Vyhledávané výrazy na internetu

V prohlížeči i ve vyhledávačích se ukládá, co uživatel hledal, co chtěl zjistit a jak tyto požadavky formuloval. Mezi nejúspěšnější vyhledávače patří Google, který dokáže vyhledávat i celé věty na internetu. A většina uživatelů hledá metodou pokus omyl. Šlo by to i jinak ale to uživatelé většinou neumí. Naštěstí jsou vyhledávače chytré a vědí, že mají brát v potaz vaši polohu a budou vám vyhledávat například kavárny ve vašem okolí a ne na druhém konci republiky.

Díky tomu že se ukládají informace, které hledáte na internetu, se vytváří žebříček nejhledanějších výrazů, a pokud předtím nějaký jiný uživatel již toto spojení hledal, zobrazí se mu v nápovědě, popřípadě pokud již toto samé hledal uživatel sám, vyskočí mu to ihned nahoře.

3.2.2.3 Informace o čase stráveném na stránce

Stránky ukládají informace o tom, jak uživatel tráví čas na daných stránkách. Zaznamenávají, odkud uživatel přišel, z jaké stránky a na jakou stránku poté pokračoval. Měří čas strávený na jednotlivé stránce, zda přečetl celý článek, nebo ho jen letmo projel. Tyto poznatky se používají při internetové reklamě. Podle počtu lidí na stránkách a době

strávené na ní, se dá určit, odměna pro provozovatele stránek, za poskytování reklamy na jeho stránkách.

3.3 Zneužití digitálních stop

Uživatelé si dost často myslí, že se jim nemůže nic stát, že jsou na internetu v bezpečí a pokud něco někam přidají „anonymně“, tak nikdo nedokáže dohledat, kdo přidal. Jakákoliv digitální stopa se dá v dnešní době zneužít, stačí jen vědět jak. Někdy ve prospěch uživatele, někdy ve prospěch toho kdo jí zneužívá.

Velkým problémem je i to že v dnešní době mnoho uživatelů mezi sebou komunikuje velmi otevřeně. Někdy až nezodpovědná komunikace, a přenos informací. A protože v prostředí internetu se nedá nic schovat, protože není kde to schovat. Těch rizik je nespočet a proto zde zmíním jen několik.

3.3.1 Sledování uživatelů

Sledovat uživatele v online prostředí jde udělat dvěma způsoby. První je navštívenou stránkou, nebo třetí stranou v zastoupení sběrateli dat, nebo reklamními společnostmi.

Webové stránky používají tyto data ke statistickým účelům. Zjišťují si návštěvnost stránek, nejčastěji navštívené stránky, nejlepší články, atd. Tyto statistiky ale nemusí předávat třetím stranám, pokud nechtějí.

Zatímco pro třetí strany je to výhodný byznys, každou získanou informaci dokážou zpeněžit. Rozvoj toho byznysu je díky velké poptávce reklamních společností, které se poptávají po těchto informacích. Tyto společnosti se snaží zlepšit svoje služby a poskytovat cílenou reklamu na uživatele, a proto je pro ně životně důležité využívat tyto informace. Jinak by to nemohlo ani fungovat, pokud by reklamní společnost neměla tyto informace, tak by nebyla schopná vytvořit reklamu cílenou na uživatele. Jakmile získají informace, vytváří profil uživatele, se kterým se dále pracuje. Využívají tyto profily k reklamním účelům, nebo k prodeji, pokud se na něj specializují a profitují z něho.

Soukromí jedince může být ohroženo, pokud se společnost nashromáždí dost informací. V těchto profilech bývají většinou uloženy informace o poloze a pohybu, pohlaví, odhad věku, zájmy, rodinný stav, popřípadě vlastnictví nemovitostí. Tyto informace sami o sobě nemusí vést k přesné identifikaci, a proto to nejsou informace osobní. Jenže pokud budeme mít dostatek informací a dokážeme je propojit s jinými informacemi, tak může dojít k identifikaci uživatele. Firmy se snaží stále využívat sofistikovanější metody.

3.3.2 Cookies

První soubory cookies se objevili v roce 1994 v prohlížeči Navigator od firmy Netscape. Do té doby byli prohlížeče bez cookies. Jakmile uživatel opustil stránku a znovu se vrátil na původní stránku, tak se začínala relace od začátku. Proto nebylo možné jednotlivé uživatele nijak rozlišovat. Ale cookies dalo možnost stránkám ukládat soubor do počítače uživatele, po většinou textový. V tomto souboru je unikátní ID a mnoho jiných důležitých informací, díky kterým je možné identifikovat jak počítač a konkrétní web. Jednoduše se to dá představit jako návštěva v čistírně. Po vstupu předáme obsluze doklad a ta vydá příslušný oděv. Díky tomu lze ukládat přihlašovací údaje například na univerzitním informačním systému. Původně byli cookies vytvořeny s dobrým úmyslem na zlepšení funkcí stránek. Zjednodušit uživatelům práci na internetu.

Cookies můžeme rozdělit na dva typy. Na ty co jsou na straně uživatele a ty co jsou na třetích stranách. Pokud je cookies uložena v počítači, tak se využívá ke komunikaci mezi počítačem a webovou stránkou. Jde o vzájemnou identifikaci, oblíbené nastavení, uložené uživatelské jméno a heslo. Ty cookies, co jsou třetích stran, dokážou identifikovat uživatelův počítač na všech webových stránkách, které spravuje daná společnost. Dokážou sledovat uživatele napříč internetem, aniž by o tom uživatel vůbec věděl. V těchto informacích se dají najít informace typu poslední navštívená stránka, čtené články, co bylo hledáno na daném webové stránce. Po zjištění těchto informací je možné složit profil uživatele. V cookies většinou nejsou osobní informace, pokud je uživatel nedá webové

stránce dobrovolně. Jakmile jsou zjištěny osobní informace lze spojit s profilem i reálnou identitu uživatele.

3.3.2.1 Flash cookies

Jedná se local shared object neboli LSO. Tento druh cookies, který je do počítače ukládán aplikacemi založenými na platformě Flash. Díky tomu to je tento název. Pomocí flashe se využívá obrázková reklama, grafická animace, reklamní bannery, jednoduché hry či videa, na jakémkoli prohlížeči. Tyto cookies jsou stejné jako normální cookies. Jakmile provede identifikaci tak spustí příslušnou činnost. Tyto cookies používá skoro polovina webových stránek. Mají však i negativní stránku. Pokud uživatel maže cookies, tak to nemá vliv na flash cookies. Flash cookies má neomezenou expirační dobu a při její velikosti zanášejí pevný disk počítače. Proto dokážou třetí strany velmi snadno sledovat pohyb uživatele napříč weby i prohlížeči.

V posledních měsících se mluvilo o tom že flash není bezpečný, jsou v něm závažné bezpečnostní chyby, které otevírají zadní vrátka útočníkům. Postupně se začalo stávat, že bezpečnostní rizika rostla, a proto se začaná od flashe upouštět. Adobe ohlásilo že končí s flashem a měl by ho časem nahradit HTML5.

3.3.3 Pixelový tag

Jedná se o malý obrázek, který je ve zdrojovém kódu webové stránky, nebo emailu. Vytváří ho buď webová stránka, na kterou přistupujeme, nebo třetí strana, přesněji jejich webová stránka. Jakmile uživatel otevře stránku s pixelovým tagem, tak prohlížeč pošle dotaz na tento tag, aby dostal odpověď, z jakého serveru pochází. Po tomto požadavku dostává vzdálený server veškeré důležité informace, které potřeboval. Ihned zjistí IP adresu uživatele, datum, čas a URL adresu webové stránky, na který je tag uložen. Ve chvíli kdy webová stránka s tagem uložené cookies v počítači uživatele, tak ji přečte a zaznamená. Existují i takové tagy, které zaznamenávají, co uživatel píše a jak jezdí kurzor myši.

3.3.4 Sociální sítě – pluginy

Nově v získávání informací se využívají sociální pluginy od sociálních sítí. Jednotlivé widgety a aplikace se objevují skoro na všech stránkách. Díky tomu je možné propojení obsahu stránky s profilem na sociální síti.

Jednou z největších sociálních sítí je Facebook. Ten sleduje uživatele, co jsou aktivní i neaktivní na facebooku dokonce i ty kteří nemají účet založený. Je jedno jestli jsou uživatelé přihlášeni na facebooku nebo ne. Stačí, jakmile se jednou stáhne cookies soubor z domény facebook.com. Poté sledují veškerý pohyb na internetu. Jakmile se uživatel připojí na stránku, kde je widget sociální sítě, tak je sledován danou sociální sítí. Ukládá se IP adresa, informace o operačním systému, verzi prohlížeče, navštívené stránky a čas, ale hlavní je anonymní, unikátní alfanumerický kód. U přihlášených uživatelů na sociální síť se místo unikátního kódu uloží profil ze sociální sítě, informace o něm ze sociální sítě.

3.3.5 Zneužití digitální identity

Jakmile útočník nashromáždí dostatek informací o uživateli, tak si dokáže vytvořit falešnou identitu, a poškodit uživatele, nebo někoho v jeho okolí. Dá se zneužít ekonomicky. Vezme si na uživatele půjčku, zadluží se. Další věcí je že poškodí dobré jméno uživatele nebo firmy, což může vést i ke zničení života a podnikání.

3.3.6 Stalking

Cyberstalking je dnes velmi rozšířený, jedná se o sledování na internetu, sledování komunikace uživatelů a využívání jí k obtěžování uživatele. Existují různá stádia při stalkingu.

Jsou dva druhy stalkingu jeden je přímý a druhý je nepřímý. V přímém cyberstalkingu jde o zastrašování, urážlivé zprávy, nebo sexuální kontext za pomoci SMS zpráv a emailu, popřípadě v chatovacích aplikacích. Druhým způsobem je nepřímý cyberctalking a jedná se o to, že útočník využívá internetu na poškození dobrého jména

uživatel, na výhružky, ale nedělá to přímo, dělá to anonymně. Většinou v diskusních fórech, chatovacích místnostech.

3.3.7 Krádež identity

Když myslíme krádež identity, tak tím myslíme, že se útočník vydává za někoho jiného, za uživatele o kterém nashromáždil dostatek informací. Tento proces má dvě části, nejdřív musí útočník uživatele sledovat, aby získal jeho osobní informace a důležité informace pro jeho plán. Druhou části je zneužití nabytých informací ve prospěch útočníka.

Na krádež identity je mnoho motivů, útočník se může vydávat za oběť, kterou uživatel poškodil, ale tím chce poškodit dobré jméno uživatele. Dalším důvodem proč to útočník dělá je proto, aby se finančně obohatil, chce ukrást uživateli jeho finanční prostředky z bankovních účtů. Nemusí profitovat pouze z bankovních účtů. Peníze lze vydělat i z prodeje osobních informací třetím stranám. Při tomto druhu útoku se útočník zaměřuje na kreditní karty, přihlašovací údaje k emalovým serverům s tím spojené adresy, na které je následně zasílán spam.

Většina lidí sdělí informace sama o sobě třetí straně dobrovolně za nějakou výhodu, například sleva v obchodním domě. Jen velmi málo lidí odmítne jakkoliv potenciálnímu útočníkovi pomoci se získáním informací o sobě. Na stránkách technet.cz byl zveřejněný test, kolik lidí příjme na sociální síti facebook přátelství od neznámé osoby. Proto vytvořili falešné profily muže a ženy. Poté rozesílali náhodně mezi uživateli žádosti. Výsledky byli velmi překvapivé, z testované skupiny byli výsledky takové, že 60 % mužů žádost od ženského profilu přijalo a 42 % žen z mužského profilu též přijalo. Tím poskytli citlivé informace třetí straně, aniž by věděli, o koho se jedná. Kdyby to nebyl test ale záměrný útok útočník by zjistil veškeré informace, co by potřeboval k útoku či prodeji. Uživatelé běžně toto praktikují i u webových stránek kde jim registrace zajistí bezplatné využití těchto stránek. Uživatel si ale neuvědomuje, že tato stránka není bezplatná, ale neplatí za ní penězi, ale informacemi o sobě. Protože těchto e-shopů, webových stránek s přihlášením, sociálních sítí je mnoho, není v možné nijak vytvořenou databázi kontrolovat. A pokud se stanou útokem hackerů, tak získají velké množství informací najednou. Tyto útoky nejsou

jednoduché a vyžadují velký výpočetní výkon a velmi dobré znalosti, proto tyto útoky dělají pouze zkušení hackeři.

Velkým problémem je i to, že uživatelé zveřejňují veškeré informace o sobě na sociálních sítích, kde je nemají nijak zabezpečeny. Takže útočník většinou nemusí mít uživatele v přátelích, aby získal tyto informace. Druhou stranou problému je i to, že sociální sítě nechrání uživatele nad rámec zákona. Takže vše co nepodléhá zákonům, je veřejné pokud to uživatel nepřenastaví jinak. Toto je velmi jednoduchý způsob jak získat informace o uživateli bez odborných znalostí.

V dnešní době není nic neobvyklého, že se objevují automatické dataminingy, které dostávají, za pomocí softwaru v počítači, informace ze sociálních sítí. Stačí mít dostatečný výkon a jde vše, co útočníka napadne. Tato metoda se používá v případech, kdy útočník chce získat velký soubor dat, ze sociálních sítí jako například facebook nebo google+. Veškeré tyto softwary se dají stáhnout na internetu, není nijak těžké je dohledat.

Ne všechny digitální stopy jsou cílem útoku, existují také kontrolní bezpečnostní otázky, které jsou též rizikem. Jedná se o otázky, které se používají při zapomenutém heslu do emailové schránky. Pokud má útočník k dispozici profil na sociální síti, není pro něj problém získat si odpovědi na tyto kontrolní otázky. Poté se naboura do emailu a uživatel to zjistí až poté co se nebude moci přihlásit. Tato metoda je i částečně o štěstí, nejde o sofistikovanou vědeckou metodu, která by měla pokaždé výsledek. Spíše o zajímavý způsob toho jak mohou být digitální stopy využity.

3.3.8 Personalistika

Nejedná se čistě o zneužití, ale personalisté využívají vyhledávání na sociálních sítích v prvních kolech pohovorů. Díky tomu zjistí personalista o uchazeči o práci často více, než by zjistil při normálních pohovoru. Nalezne jeho zájmy, koníčky, názory, následně z toho dokážou vytvořit profil uchazeče o práci, ještě před prvním kontaktem. Zjistí, jak se dokáže uchazeč vyjadřovat v diskuzi, jestli dokáže logicky a věcně argumentovat svojí pravdu, či nikoli. Následně personalista vyhledává informace, které by mu pomohli určit, jestli se k nim do firmy hodí nebo ne, tyto informace mu pomohou se

rozhodnout, jestli ho přijmou nebo ne. Hlavním pravidlem je, že co je na internetu nejde už vzít zpět. Mnoho personalistů odmítne uchazeče jen na základě sdílených fotografií na sociálních sítích nebo komentářích na nich.

Na internetu platí pravidlo, že uživatel by neměl sdílet nic, co by neřekl v reálném životě. Tím se bohužel uživatelé moc neřídí. Naštěstí uživatelé začínají chápat, že chování v online prostoru vytváří jejich obraz v reálném světě. Proto uživatelé začínají upravovat svoje profily na sociálních sítích, aby zlepšili svůj profil, své digitální stopy.

3.4 Rozsah stop

Na kontrolu digitálních stop existuje mnoho nástrojů. Nejjednodušší co může uživatel udělat je nepoužívat internet a komunikační technologie. Toto řešení není v dnešní době použitelné, pokud zvážíme, že každý člověk na planetě využívá tyto technologie na komunikaci, při práci. Člověk je s nimi v každodenním spojení a nedokáže si představit, že by je musel opustit. I když použijeme vhodné nástroje tak nikdy nedosáhneme úplně stoprocentních výsledků. Důležitou otázkou je jak ta digitální stopa, kterou člověk má vypadá.

3.4.1 Aktivní stopy

Jednoduchý způsob jak zjistit svoje digitální stopy je zadat si svoje jméno do vyhledávače prohlížeče. A hledat informace o sobě. Pro specifičtější vyhledávání můžeme použít ke jménu i email, telefonní číslo, přezdívku na fórech, atd.

Jakmile ostraníme nerelevantní výsledky, které jsou způsobeny stejnými jmény. Dohledáme se možného rizika a z toho lze vyvodit závěry, toho jak zmenšit digitální stopy co uživatel zanechává.

3.4.1.1 People search engine

Jedná se o specifický nástroj na vyhledávání své digitální stopy. Jedná se o specifičtější a sofistikovanější způsob, než pomocí vyhledávače v prohlížeči. Hlavní

výhodou je že uživatel nedostane odkazy, ale namísto toho dostane ucelenou tabulku informací. Uvedu zde dva zástupce těchto technologií.

Prvním zástupcem je People Finders. Je to velmi účinný nástroj, který dokáže najít i trestné činy v databázi, čímž zjistí kriminální minulost hledané osoby. Jediná nevýhoda je, že funguje jen v USA.

Dalším zástupcem je Pipl, který po zadání konkrétních informacích prohledá internet a nalezne, co se dá na osobu, kterou uživatel vyhledává. Projede stránky, které roboti vyhledávačů nechtějí vidět.

3.4.1.2 Google Dashboard

Jedná se o nástroj od společnosti Google, který ukazuje digitální stopu uživatele na produktech od firmy Google. Jsou to služby jako Gmail, Picasa, Fotky, Historie polohy,… Uživatel tak dostává plný přehled o tom, co vše využívá u společnosti Google a jaké má digitální stopy. Dá se zde dohledat i poloha a místa, která člověk navštívil.

V této službě máme i možnost nastavení jednotlivých aplikací, které uživatel využívá.

3.4.1.3 Google Ad Preferences

Tento nástroj umožňuje upravovat profil, který cílí reklamní sdělení na uživatele. V tomto nástroji může uživatel upravit reklamu, kterou bude od společnosti dostávat při vyhledávání, popřípadě upravit co chce vidět. Tento nástroj má dvě podmínky. Uživatel musí mít jeden účet u služeb, které poskytuje společnost Google a povolení přijímání cookies od třetích stran.

V tomto nástroji nenajde uživatel celkovou digitální stopu ale jen částečnou, ale vidí, jak vypadají zájmové profily u reklamních společností.

3.5 Správa stop

Své aktivní digitální stopy lez docela jednoduše spravovat. Záleží na tom, jak se uživatel chová na internetu. Nejlepší je prevence. Je třeba, aby si uživatel uvědomil, kde a jak svá data zveřejňuje. Jakmile se někam jednou ty data dostanou, tak už se nedají vzít zpět. Můžou způsobit uživateli velké problémy. Problémům jde předejít tím, že uživatel nebude do budoucna nic publikovat. Jenže jakmile toto začne praktikovat, tak nevyužije plný potenciál webových služeb. Nemůže ale počítat že vše bude fungovat na 100 %.

Základním předpokladem minimalizace digitálních stop je využívat bezpečnostní zásady. Jedním ze základních je přihlášení více uživatelských jmen na internetu, dalším je zvažovat co kde a jak uživatel zveřejní, fotografie, videa. Dalším je vhodné nastavení soukromí a soukromé zabezpečené prohlížení.

3.5.1 Více uživatelských jmen

Základem je využívání více přezdívek na internetu, na více službách. Není dobré používat jednu přezdívku napříč internetem. Díky tomu že nebude uživatel používat jedno uživatelské jméno, tak nebude pro reklamní společnosti tak jednoduché udělal profil uživatele. A nedostanou citlivé informace.

3.5.2 Publikace fotografií, videí

Jde o to, že uživatelé dnes zveřejňují na internet, kde co a ne dokážou si představit, jaké by to mohlo mít následky. Proto je dobré, aby uvážil, co nahrává a jak citlivé informace s tím sděluje. Uživatel by si měl zkontrolovat, zda nejsou jeho data předávána dál.

3.5.3 Soukromí

Každý uživatel by si měl nastavit své soukromí tak, aby nezveřejňoval příliš informací sám o sobě, popřípadě o svých známých. Uživatel ovlivní, jak moc bude k vyhledání.

3.5.4 Zabezpečení

Jedná se o to, že je potřeba aby uživatel průběžně mazal své soubory cookies, aby nedával příležitost nechávat se sledovat. Díky tomu ho nebudou moci tolik sledovat třetí strany. Je třeba spravovat veškeré soubory, co ukládá prohlížeč a mazat ty co nejsou potřeba.

Služba, která dokáže sledovat uživatelovy digitální stopy, se nazývá Me on the Web. Je to služba, která se nachází v již zmíněném Google Dashboard. Jedná se o monitorovací nástroj, který vyhledává nové informace o uživateli v přesně vymezeném rozsahu, podle zadaných klíčových slov. Jakmile robot najde informaci o uživateli, tak dostane uživatel mail s touto shodou. Díky tomu dostane uživatel ihned zpětnou vazbu a možnost kontroly svých stop. Jedinou nevýhodou je to že je to alertová služba, která prochází pouze viditelný web. Proto nedokáže objevit všechny stopy.

Primárně se vyhledává jméno a email uživatele, v dalších nastaveních lze nastavit přezdívka, telefonní číslo a další emailové adresy. Díky tomu zahrne do vyhledávání další informace. A vyhledávání je přesnější. Dále lze nastavit interval upozornění. Záleží na tom, jestli uživatel chce mít informace každý den, týden, měsíc, nebo jen když se objeví nová stopa.

Uživatel si může zvolit tyto služby i u dalších velkých vyhledávačů, jako například Bing. Výrazně se ale výsledky lišit nebudou. Zmíněná tato služba byla díky tomu, že je uváděna jako nástroj na správu své digitální stopy.

4 Vlastní práce

V dnešní době je velké množství nástrojů na odhalování, skrývání digitálních stop. V této části provedu test několika vybraných programů. Celé testování bude na virtuálním stoji, na to použiji Virtualbox do kterého nainstaluji Windows 7 32 bitů. Protože, nelze všechny programy hodnotit jednotlivě udělám si 3 kategorie, ve kterých je budu testovat. Jednotlivé typy se od sebe liší tím, jestli to jsou programy, pluginy. Proto si to rozdělíme na nástroje, které zabraňují sledovat aktivitu, dále na nástroje které zajišťují anonymitu na internetu a nástroj na odstranění uložených sledovacích zařízení.

Budu postupovat podle přesně daného postupu, který si přiblížíme níže. Tím zajistím, aby test byl vždy stejný a nemohl být nijak ovlivněný.

Nainstaluji vždy čistý Windows 7 poté prohlížeč Mozilla Firefox v nejnovější verzi. Nainstaluji příslušný nástroj a provedu nastavení. Poté začnu navštěvovat webové stránky v přesném pořadí.

4.1 Nástroje zabraňující sledování

Pokud uživatel chce, a obává se o svoje soukromí, tak může využít nástroje na zabránění sledování aktivit. Tyto nástroje nepotřebují po uživateli žádné další nastavení. Když vezmeme v úvahu jednoduchost a požadavky tak je to vhodné nástroje pro většinu uživatelů, kteří nejsou tak zkušení.

4.1.1 TrackerBlock

Tento nástroj je dostupný ve více prohlížečích. Nejen na testovaném prohlížeči Mozilla Firefox. Pro to aby nemohli uživatele sledovat, tak využívá čtyři nástroje.

Prvním nástrojem je nastavení hlavičky DNT, která říká společnostem, že uživatel nechce, aby ho společnosti sledovali. Dalším nástrojem je ochrana cookies. Dělá to tak, že zabraní číst, upravovat a zapisovat do cookies. Další je tzv. Opt-out cookies. Tento nástroj nastaví vymazání cookies ze serverů společnosti a tím zabrání reklamě. Posledním nástrojem je ochrana HTML5. Specifika toho nástroje umožňují, aby stránky ukládali

informace podobné cookies, ale nejsou to cookies, které pomáhají načítání stránek. Společnosti ale této možnosti zneužívají. A proto tento nástroj dokáže najít, zda se ukládají cookies nebo ne.

Jedná se sice rozmanitý nástroj, ale zabezpečuje pouze pasivní stopy. Není sice odolný proti jiným útokům, ale je oproti ostatním výhodnější díky HTML5 nadstavbě a také mazání flash při skončení.

Velkou výhodou je, že vše běží na pozadí a uživatel nemusí nic nastavovat a řešit. A pokud by chtěl tak má rozmanité nastavení.

4.1.2 Ghostery

Je k dostání na všechny prohlížeče, které se dají pořídit. Ve své databázi mají více než 1 000 subjektů, které jsou aktualizovány. Tento nástroj stojí na pomezí uživatelů, vládou a společnostech, které poskytují reklamu, a proto uživatel dostane na výběr, jestli chce blokovat sledování, či nikoliv. Uživatel je nejprve informován a pak se rozhodne.

Vše funguje tak, že tento nástroj detekuje neviditelné sledovací zařízení, a proto dokáže objevit zařízení jako je obrázkové objekty, což sou pixelové tagy, dále Iframes. Iframes je vložený rám s reklamou, která je vnořená. Dále nalezne vložené objekty a tagy, zabraňuje přesměrování, které uživatel nechce. Mimo jiné i dynamicky generované elementy přes JavaScrip a cookies.

Vše zde působí jako aktivní ochrana. Problém je že vše zablokuje na úrovni zdrojového kódu a to může narušit chod stránek. Naštěstí lze povolit určité prvky na stránce a tím dostat plnou funkčnost.

4.1.3 Do Not Track+

Tento nástroj je podobný, jako Ghostery. Je dostupný pro všechny dostupné internetové prohlížeče. Má vlastní databázi 600 subjektů. Neumí smazat cookies, ale dá na veškerou komunikaci hlavičku DNT. Dokáže i zablokovat sledovací zařízení a popřípadě je pak povolit.

4.1.4 Porovnání

V závěru této kapitoly vezmeme dva podobné nástroje a porovnáme je mezi sebou. K tomuto využijeme nástroj Do Not Track+ a Ghostery a proto jsem se rozhodl, že porovnám, kolik sledovacích zařízení je na testovaných stránkách. Na vybraných 10 stránkách v české republice. A pět ve světě. Vše jsem testoval na novém stroji, abych neovlivnil výsledky.

Doména	Ghostery	Do Not Track+	Rozdílných zařízení
Seznam.cz	1	0	1
Idnes.cz	3	3	4
Centrum.cz	4	2	2
Lide.cz	1	0	1
Stream.cz	0	0	0
Aukro.cz	4	2	4
Estranky.cz	4	3	3
Invia.cz	3	1	2
Blog.cz	4	4	0
Csfd.cz	3	1	2
Google	0	0	0
Facebook	0	0	0
youtube	1	2	2
Yahoo!	1	2	1
MSN	4	8	4
Celkový počet nalezených zařízení	33	28	
Vítězství nad nástrojem	7	3	

Tabulka 1 - Ghostery vs. Do Not Track+

Ghostery nalezlo více zařízení a vyhrálo nad svým oponentem o čtyři. Celkové skóre bylo sedm vítězství pro postery a tři pro Do Not Track+. V pěti případech to bylo nerozhodně. Ghostery celkově nalezlo 33 sledovacích zařízení a Do Not Track+ nalezlo 28 zařízení.

Rozdíly nebyl jen v počtu nalezených stop, ale hlavně v nalezených sledovacích zařízeních. Vše záleží na tom, jakou databázi používají. Tyto dva nástroje se vzájemně doplňují, a protože mohou běžet bez rozporu spolu, tak se jedná a o ideální kombinaci proti sledování.

4.2 Nástroje na anonymitu na internetu

Jedním z nástrojů jak chránit své stopy, je zakrývat, co děláme na internetu, zajistit si anonymitu. Tady budeme testovat dva nástroje a to TOR a JonDonym, které dokáží maskovat aktivity na internetu. Existují i jiné způsoby, jako například anonymní prohlížení co umožňují prohlížeče, ale to se jen tváří, jako anonymní prohlížení. Neukládají pouze historii.

4.2.1 TOR

Na testování jsme si museli stáhnout poslední verzi nástroje TOR. Funguje tak, že má část klienta a speciální upravené prohlížeč postavený na Firefoxu. Veškerá komunikace probíhá přes několik proxy serveru. To zajistí anonymitu identity. Dále se používají pluginy HTTPS Everywhere, který na všech stránkách nastaví zabezpečené prohlížení, pokud to ta stránka umožňuje. Současně zabraňuje flashování a scriptování. Díky tomuto je ochrana uživatelů na vysoké úrovni. Každých deset minut se mění identita, ale jde to dělat i ručně dříve. Díky tomu není možné, aby uživatele sledoval poskytovatel internetu. Pro všechny uživatele je jednotný jazyk a typ prohlížeče, proto nelze uživatele nijak rozeznat.

Your IP	93.182.129.86 (Tor)	Traceroute
Your location	Skane Lan, Lund	Show on map
Your net provider	Infra-trygg	Whois IP
Reverse DNS	exit3.ipredator.se	Whois Domain

Attribute	Value	Rating
Cookies	Your browser does not store any cookies.	good
Authentication	protected	good
Cache (E-Tags)	Your unique ID: 397151197	bad
HTTP session	10 minutes (until your Tor identity is changed)	medium
Referer	Original: Websites may see from which other website you come from!	medium
Signature	8ab3a24c55ad99f4e3a6e5c03cad9446 (Firefox)	good
User-Agent	Mozilla/5.0 (Windows NT 6.1; rv:10.0) Gecko/20100101 Firefox/10.0	good
Language	en-us,en;q=0.5	good
Charset		medium
Content types	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8	good
Encoding	gzip, deflate	good
Do-Not-Track	protected	good

JavaScript	JavaScript is currently turned off.	good
Browser window	1280 x 632 pixels (inner size)	medium
Fonts	Do you see strange symbols here? If yes, your fonts are readable!	good
Browser history		good

Obrázek 1 - Výsledky nástroje TOR

4.2.2 JonDonym

Jedná se o druhého zástupce této kategorie. V testech dopadl nejlépe. Ve verzi JonDoFox je v základu slušně vybaven čtyřmi nástroji. Prvním z nich je NoScript, další je HTTPS Everywhere, cookies monster, který zajišťuje správu více druhů cookies. Posledním nástrojem je AdBlock+ zajišťující blokování reklamy a reklamních banerů. Oproti TORu blokuje i ukládání sledovacích zařízení do počítače. Nedokáže sice falšovat rozlišení, které má uživatel natavené na monitoru, ale to není nijak nebezpečná informace. Jak JonDonym tak TOR mají bezpečné vyhledávání pomocí DuckDuckGO a StartPage.

Your IP	212.117.177.5 (JonDonym)	Traceroute
Your location	Luxembourg	Show on map
Your net provider	root SA	Whois IP
Reverse DNS	anonymization-service.ya-trade.com	Whois Domain

Attribute	Value	Rating
Cookies	Your browser does not store any cookies.	good
Authentication	protected	good
Cache (E-Tags)	protected	good
HTTP session	stateless	good
Referer	hidden (changed when switching the website)	good
Signature	8ab3a24c55ad99f4e3a6e5c03cad9446 (Firefox)	good
User-Agent	Mozilla/5.0 (Windows NT 6.1; rv:10.0) Gecko/20100101 Firefox/10.0	good
Language	en-us	good
Content types	text/html,application/xml,*/*	good
Encoding	gzip, deflate	good
Do-Not-Track	protected	good

JavaScript	JavaScript is currently turned off.	good
Browser window	1280 x 612 pixels (inner size)	medium
Fonts	Do you see strange symbols here? If yes, your fonts are readable!	good
Browser history		good

Obrázek 2 - Výsledky JonDonym

4.2.3 JonDonym vs. TOR

Z testovaných zařízení vychází lépe JonDonym, který má nástroji TOR lehce navrch v kategorii e-tags a v oblasti hlavičky referer. Nedá se říci, že by nějak pohořeli, to ne, ale přeci jen je na tom JonDonym o trochu lépe. Ve prospěch JonDonym mluví i to, že veškerá komunikace je přes uzly, které jsou ověřený certifikačními autoritami. Zatím co v síti TOR je vedena komunikace přes jednotilivé počítače, to jsou uzly sítě. To představuje potenciální riziko.

	TOR	JonDonym
IP Adresa	ANO	ANO
Poskytovatel připojení	ANO	ANO
Geografická poloha	ANO	ANO
Prohlížeč	ANO	ANO
Java	ANO	ANO
Flash	ANO	ANO
Cookies	ANO	ANO
e-tags	NE	ANO
Historie	ANO	ANO
Referer	NE	ANO
Výsledky	80 %	100 %

Tabulka 2 - TOR vs. JonDonym

4.3 Nástroje na odstranění sledovacích zařízení

V této kapitolce se budeme zabývat nástroji, které dokážou odstranit sledovací zařízení z počítače. Popřípadě z prohlížeče v počítači. Hlavní nástroj pro sledování jsou soubory cookies. Pokud uživatel nepoužívá žádný z výše uvedených nástrojů, je potřeba aby si své cookies mazal sám. Všechny prohlížeče tuto možnost nabízejí. Lze nastavit, jestli se bude mazat po každém ukončení prohlížení, nebo to dělá uživatel ručně. Jenže neodstraňuje cookies typu Flash, obrázkové objekty.

Pokud chce uživatel, aby se jeho soubory mazali automaticky, tak je potřeba aby si nainstaloval nějaký speciální nástroj. Pro porovnávání jsem zde zvolil 2 nástroje, které jsem našel podle recenzí, a zároveň jsou dostupné zdarma. Prvním je CCleaner a druhým je Temp File Cleaner. (Softpedia)

4.3.1 CCleaner

Používám CCleaner v nejnovější verzi od společnosti Piriform. Jedná se o jeden z nejoblíbenějších nástrojů. Je oblíbený díky své jednoduchosti, účinosti, uživatelské přívětivosti a hlavně kvůli komplexnímu řešení, které nabízí. Tento nástroj dokáže mazat nepotřebné systémové soubory, dočasné soubory a plně se postará o soubory, které vytváří prohlížeče. Dokáže spolupracovat se všemi prohlížeči napříč platformami. Bezpečně maže informace o historii prohlížení, stahování, před vyplněné formuláře, hesla a co je ještě víc důležité, tak jsou veškerá cookies. Další výhodou u tohoto nástroje je možnost vytvořit si chráněné cookies, které se nebudou mazat. Například se to dá použít na školním univerzitním systému, kde si uživatel nechá před vyplněné přihlašovací údaje. Popřípadě nějaká vlastní nastavení na nějaké webové stránce.

4.3.2 Temp File Cleaner

Opět použijeme nejnovější verzi tohoto nástroje. Tento nástroj nabízí stejnou škálu služeb, jako CCleaner. Dokáže také odstraňovat informace, které ukládají prohlížeče.

Poskytuje i mazání flash cookies a historie prohlížení, historie vyhledávání. Bohužel tento nástroj neumožňuje nastavení výjimek na určité mazací nástroje.

4.3.3 CCleaner vs. Temp File Cleaner

Oba dva testované nástroje mají shodné parametry a výkony. Jediné v čem se liší, je že Temp File Cleaner nedokázal odstranit Silverlight cookies. CCleaner dokázal odstranit vše, co se používá na sledování uživatelů. V kombinaci toho, že je velmi uživatelsky přívětivý a jednoduchý, tak je ideální nástroj pro nenáročného uživatele. Temp File Cleaner skončil hned za CClerem. Konkuruje velmi zdárně, ale přeci jen není tak dobrý jako CCleaner. Hlavním mínusem je to že nemá seznam vyjímek.

Kriteria	CCleaner	Temp File Cleaner
Cookies	ANO	ANO
Historie prohlížení	ANO	ANO
Cashe	ANO	ANO
Flash cookies	ANO	ANO
Silverlight cookies	ANO	NE
Celkem	100 %	80 %

Tabulka 3 - CCleaner vs. Temp File Cleaner

5 Závěr

Podařilo se mi charakterizovat digitální stopy, které zanechává uživatel ať vědomě či nevědomě. Představil jsem zde i možnosti ochrany uživatele před uchováváním digitálních stop. Toto téma je v dnešní době dosti aktuální, a nemyslím si, že by někdy přestalo. Uživatelé pořád rozlišují mezi bezpečím v online světem a v reálném životě, zatím si to nespojují. Ale bohužel to tak není, naše digitální identita je velmi důležitá.

Cílem práce bylo charakterizovat jednotlivé digitální stopy. S tím související nalezení ochrany proti zneužití digitálních stop. Dílčími cíly bylo nalezení a test nástrojů se schopností maskovat uživatele na internetu. Dále nalezení nástroje na objevování uložených digitálních stop v počítači od třetích stran. Testoval jsem i nástroje, které zabraňují sledování uživatele na internetu.

V této práci byly představeny typy digitálních stop. Rozdělení na aktivní a pasivní digitální stopy. V každé kategorii je několik unikátních kategorií, o kterých zde bylo hovořeno.

Pokud uživatelé požadují úplnou anonymitu tak by měli využívat služeb anonymních sítí jako například TOR či JonDonym. Při využívání těchto sítí, ale může dojít k tomu, že některé webové služby nebudou dostupné, popřípadě omezené. Jakmile bude stránka využívat flash či Javu, bude zobrazení stránek omezené.

Pokud uživatel nechce, aby měl omezené služby tak existují i jiné nástroje, které toto nedělají. Zástupce těchto nástrojů jsou Ghostery a Do Not Track+, využívají k tomu nastavení hlavičky DNT. Jsou dostupné na mnoha platformách. Nejsou tak výkonné jako anonymní sítě, odhalují jen některé hrozby, ale nenarušují fungování webových stránek. Naštěstí se dají volně kombinovat

Třetí testovanou kategorii jsou nástroje na odstranění sledovacích zařízení v počítači. Dnes se dá sehnat dostatek softwaru, který to udělá za uživatele jednoduše a bez práce.

Z testování nejlépe vyšel program CCleaner, který odstranil vše nebezpečné. Druhý testovaný produkt Temp File Cleaner, ten byl v testu též úspěšný, ale ne tak jako jeho kolega.

V dnešní době existuje mnoho nástrojů, které se dají použít. Důležité je aby uživatel měl alespoň něco ve svém počítači. Veškeré nástroje se dají sehnat bezplatně, a proto není pro uživatele problém si je pořídit. Vhodná je kombinace více nástrojů současně.

6 Seznam použitých zdrojů

6.1 Literatura

DOSEDĚL, Tomáš. 2004. *Počítačová bezpečnost a ochrana dat*. Vyd. 1. Brno: Computer Press. ISBN 80-251-0106-1.

ECKERTOVÁ, Lenka a Daniel DOČEKAL. 2013. *Bezpečnost dětí na internetu: rádce zodpovědného rodiče*. 1. vyd. Brno: Computer Press. ISBN 978-80-251-3804-5.

FISH, Tony. 2009. *My digital footprint: a two-sided digital business model where your privacy will be someone else's business!*. London: Futuretext. ISBN 978-0-9556069-8-4.

MATOUŠOVÁ, Miroslava a Ladislav HEJLÍK. 2008. *Osobní údaje a jejich ochrana*. 2., dopl. a aktualiz. vyd. Praha: ASPI. Právní rukověť (ASPI). ISBN 978-80-7357-322-5.

6.2 Internet

ČERNÝ, Michal. Digitální stopy. In: *E-bezpečí* [online]. 2011 [cit. 2016-03-14]. Dostupné z: http://www.e-bezpeci.cz/index.php/temata/sociotechnika/312-digitalni-stopy

DOČEKAL, Daniel. Google Profiles nabízejí miliony jmen i e-mailů uživatelů. *JustIT* [online]. 26/05/2011 [cit. 2016-03-14]. Dostupné z: http://www.justit.cz/wordpress/2011/05/26/google-profiles-nabizeji-miliony-jmen-i-e-mailu-uzivatelu/

DOČEKAL, Daniel. Hacknutý web ODS a data o členech z něj získaná podruhé. *Pooh* [online]. 2012 [cit. 2016-03-14]. Dostupné z: http://pooh.cz/pooh/a.asp?a=2017672

E-bezpečí. *E-bezpečí* [online]. 2015 [cit. 2016-03-11]. Dostupné z: https://wikisofia.cz/index.php/Cyberstalking

E-bezpečí: Digitální Stopy. *E-bezpečí* [online]. 2011 [cit. 2016-03-11]. Dostupné z: http://www.e-bezpeci.cz/index.php/temata/sociotechnika/312-digitalni-stopy

Informační bezpečnost: Ochrana osobních údajů na internetu. *Elektra*: *Portál elektronických materiálů FF UK* [online]. 2011 [cit. 2016-03-14]. Dostupné z: http://elektra.ff.cuni.cz/ingram/informacni-bezpecnost/InfoBezpecnost.pdf

Ochrana soukromí v praxi. *Ludvig von Mises institut* [online]. [cit. 2016-03-14]. Dostupné z: http://www.mises.cz/clanky/ochrana-soukromi-v-praxi-1026.aspx

Softpedia. *Softpedia* [online]. [cit. 2016-03-14]. Dostupné z: http://www.softpedia.com

Technet. *Technet* [online]. 2009 [cit. 2016-03-11]. Dostupné z: http://technet.idnes.cz/cesi-facebooku-nebezpecne-veri-falesne-krasavici-naletelo-60-procent-112-/sw_internet.aspx?c=A091117_171036_sw_internet_pka

Wikisofia: Digitální stopa. *Wikisofia* [online]. [cit. 2016-03-11]. Dostupné z: https://wikisofia.cz/index.php/Digit%C3%A1ln%C3%AD_stopa