Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Digitální stopa na Internetu

Vojtěch Sloup

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Vojtěch Sloup

Informatika

Název práce

Digitální stopa na Internetu

Název anglicky

Digital footprint on the Internet

Cíle práce

Cílem bakalářské práce je analyzovat problematiku digitální stopy z hlediska serverů, síťových prvků a koncových stanic a přehledným způsobem zpracovat shrnutí hrozeb vyplývajících z výsledků předchozí analýzy. Dílčím cílem práce je na základě získaných poznatků stanovit opatření a určit vhodné nástroje k eliminaci vzniklé digitální stopy.

Metodika

Teoretická část práce bude zpracovávat problematiku digitální stopy v prostředí Internetu. Zdrojem informací bude vědecká a odborná literatura a odborné články. Doplňkovým zdrojem budou internetové články

Syntetická část práce bude obsahovat návrh opatření a určovat vhodné nástroje k eliminaci vzniklé digitální stopy za účelem zvýšení bezpečnosti a ochrany soukromí uživatelů internetu.

Doporučený rozsah práce

30 – 40 stran

Klíčová slova

Bezpečnost, internet, ochrana soukromí, osobní informace

Doporučené zdroje informací

ČERNÝ, Michal. Digitální stopy a digitální identita. RVP: Metodický portál [online]. 2011. Dostupné z: http://clanky.rvp.cz/clanek/o/g/12943/DIGITALNI-STOPY-A-DIGITALNI-IDENTITA.html

GARFINKEL, Simson a Gene SPAFFORD. Web security & commerce. Cambridge: O'Reilly & Associates, c1997, xx, 483 s. ISBN 1565922697.

GRAYSON, Robert. Managing your digital footprint. 1st ed. New York: Rosen Central, 2011, 48 s. Digital and information literacy. ISBN 978-1-4488-2296-6.

KRÁL, Mojmír. Bezpečný internet: chraňte sebe i svůj počítač. První vydání. Praha: Grada Publishing, a.s., 2015, 183 stran. Průvodce (Grada). ISBN 978-80-247-5453-6.

MATES, Pavel. Ochrana osobních údajů. Vyd. 1. Praha: Karolinum, 2002, 73 s. ISBN 80-246-0469-8.

Předběžný termín obhajoby

2014/15 LS – PEF

Vedoucí práce

Ing. Václav Lohr, Ph.D.

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 02. 03. 2016

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Digitální stopa 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 literatury na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 11. 03. 2016 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Václavu Lohrovi, PhD., za jeho čas a ochotu, se kterou se mi věnoval a také za odbornou pomoc a konzultaci při psaní této bakalářské práce.

Digitální stopa na Internetu

Souhrn

Tato práce se zabývá problematikou digitální stopy na internetu z pohledu vzniku digitální stopy, možnosti zneužití a ochrany uživatelů internetu. Teoretická část je zaměřena na analýzu problematiky digitální stopy a zpracovává možnosti zneužití a hrozeb, vyplývajících z předchozí analýzy. Syntetická část práce obsahuje možnosti ochrany soukromí uživatelů internetu, návrhy opatření a vhodné nástroje pro eliminaci vzniklé digitální stopy.

Klíčová slova: Internet, soukromí, bezpečnost, digitální stopy, osobní informace, počítačová kriminalita, hrozby, sociální síť

Digital footprint on the Internet

Summary

This work deals with the digital footprint on the Internet in terms of creation of digital footprints, the possibility of abuse and protection of Internet users. The theoretical part is focused on analysis of digital footprint and handles the potential for abuse and threats arising from the previous analysis. Synthetic part contains options privacy of Internet users, draft measures and appropriate instruments to eliminate the resulting digital footprint.

Keywords: Internet, privacy, security, digital footprints, personal informations, cybercrime, threats, social network

Obsah

Seznam obrázků

1 Úvod

Zatímco v roce 2000 mělo přístup k internetu asi 400 milionů lidí, tak koncem letošního roku je odhadován počet on-line uživatelů na 3,2 miliardy[1]. Avšak ani tento počet není zdaleka konečným číslem. Řada soukromých firem, jako je Google nebo Facebook, připravuje projekty, které mají dostat internet i do odlehlejších oblastí[2].

Od roku 2004, kdy byl pevný obsah webových[3] stránek nahrazen prostorem pro sdílení a společnou tvorbu obsahu, označován také jako web 2.0[4], se stal pouhý uživatel i částečným tvůrcem obsahu webu.

Z těchto faktů vyplývá, že množství volně dostupných informací neustále roste a málokdo si uvědomuje, kolik a jakých informací o sobě na internetu zanechává, ať už úmyslně, či nevědomě. Je třeba zdůraznit a uvědomit si, že internet již dávno není anonymní[5].

---

[1] ICT Facts and Figures – The world in 2015. *ITU* [online]. 2015 [cit. 2015-11-19]. Dostupné z: http://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx

[2] VŠETEČKA, Roman. Do konce roku bude k internetu připojena téměř polovina obyvatel Země.*Technet.cz* [online]. 1999, 27. května 2015 [cit. 2015-11-19]. Dostupné z: http://technet.idnes.cz/celosvetove-pripojeni-k-internetu-dtx-/sw_internet.aspx?c=A150527_114416_sw_internet_vse

[3] Web - zkráceně World Wide Web (Celosvětová síť)

[4] O'REILLY, Tim. What Is Web 2.0. *O'reilly* [online]. 2005 [cit. 2015-11-19]. Dostupné z: http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html

[5] HEIN, Jakub. Internet už dávno není anonymní. In: *CCIZ* [online]. 2013, 6.2.2015 [cit. 2016-01-17]. Dostupné z: https://www.investigace.cz/internet-uz-davno-neni-anonymni

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem bakalářské práce je analyzovat problematiku digitální stopy a přehledným způsobem zpracovat shrnutí hrozeb, vyplývajících z výsledků předchozí analýzy.

Dílčím cílem práce je, na základě získaných poznatků z předchozí analýzy, stanovit opatření a určit vhodné nástroje pro částečnou nebo úplnou eliminaci vzniklé digitální stopy.

2.2 Metodika

Na začátku je definován pojem digitální stopa a zkoumán z několika úhlů pohledu, v závislosti na vzniku a typu uložení digitální stopy. Následně jsou popsána možná rizika, která vznikají spolu s digitální stopou, s ohledem na obor, který ji využívá. Tato metodika je založena na studiu odborné literatury, článků a dalších odborných materiálů.

Na základě těchto poznatků jsou popsány metody kontroly vlastní digitální stopy a k tomu doporučené nástroje. Dále jsou stanovena vhodná opatření a nástroje k eliminaci vzniklé digitální stopy za účelem zvýšení bezpečnosti a ochrany soukromí uživatelů.

3 Teoretická východiska

3.1 Druhy a typy digitálních stop

Jakákoliv aktivita spojená s internetem, počítačem, mobilem dokonce i s televizí, zanechává určitá data či metadata[6] (data o datech), která o nás vypovídají nemálo informací. Televize může zaznamenávat data o preferenci programů, době sledování nebo například přítomnosti u přijímače (což se dá odvodit z přepínání programů či rychlého přetáčení). Při používání internetu po nás zůstávají data úmyslně vytvořená (příspěvky v diskuzích či sociálních sítích, vkládání obrázků či souborů, vyplňování formulářů při nakupování v elektronických obchodech nebo i tvorba vlastních webových stránek či blogů) nebo nevědomě shromažďovaná (navštěvované stránky a dobu navštívení, vyhledávané výrazy, pravopis, stahované soubory, jaký používáme prohlížeč či operační systém)[7]. Mobilní zařízení rozšiřují tato data o typ zařízení, polohu, jaké aplikace používáte, koho máte v kontaktech, odkud a kam jezdíte či kde bydlíte a kde pracujete[8].

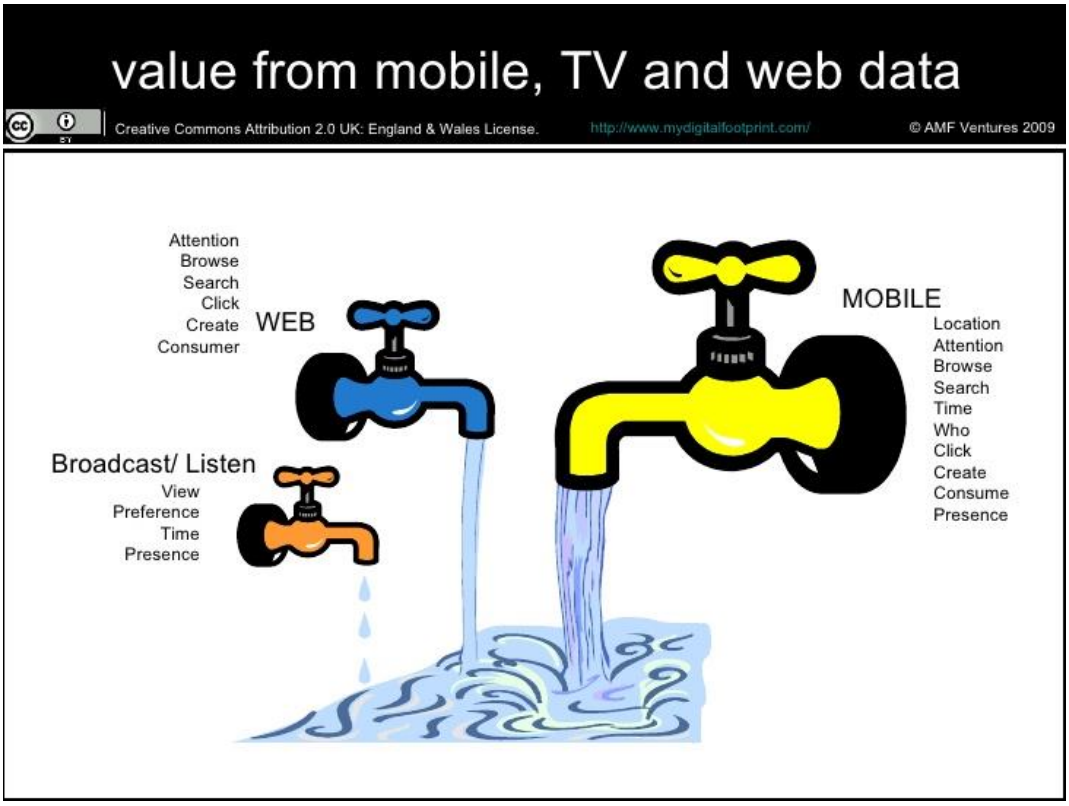
Objem dat, který po sobě zanecháváme, ilustruje obrázek 1. Jednotlivé kohoutky znázorňují zařízení a proud vtékající vody pak množství dat, kterým naplňují pomyslnou nádrž znázorňující celkový objem digitálních dat, která jsou o nás ukládána na základě našich interakcí.

---

[6] ROUSE, Margaret. Metadata. In: *Whotis.com* [online]. 1999, červenec 2013 [cit. 2016-01-17]. Dostupné z: http://whatis.techtarget.com/definition/metadata

[7] TONY FISH. *My digital footprint: a two sided digital business model where your privacy will be someone else's business* [online]. London: Futuretext, 2009 [cit. 2016-01-17]. ISBN 09-556-0698-5.

[8] NOVÁK, Michal. Jaké informace o vás Google shromažďuje. In: *SPRÁVA-SÍTĚ.com* [online]. 2016, 7.9.2015 [cit. 2016-01-17]. Dostupné z: http://www.sprava-site.com/jake-informace-o-vas-google-shromazduje-2353



Obrázek 1 – Objem dat podle typu zařízení
Zdroj: http://www.slideshare.net/tonyfish/my-digital-footprint

Všechna tato data se dají označit za digitální stopy. Vzhledem k množství druhů a typů digitálních stop se zaměříme pouze na data, tedy digitální stopu, kterou za sebou zanecháváme při používání internetu. Rozdělíme je na snadno vyhledávatelné a veřejné, s omezeným přístupem a zcela skryté.

3.1.1 Snadno vyhledávatelné a veřejné

Mezi největšího sběratele digitálních stop patří Google. Už jen tím, že jeho prostřednictvím vyhledáváme, si o nás ukládá data, která se postupně spojují a vytvářejí ucelenější představu o tom, co máme rádi, co děláme, co nakupujeme a čím víc služeb používáme, tím přesnější data o nás má. Přihlášením z počítače si Google může zaznamenat jako první informaci IP adresu, ze které se počítač na internet přihlásil. Podle té zjistí, odkud uživatel pochází. Google analyzuje například to, jaké stránky

navštěvujeme, eviduje také věk, pohlaví či zájmy uživatelů[9]. V určitém rozsahu se tato data dají získat obyčejným vyhledáváním.

Dalším, avšak neméně důležitým zdrojem dat jsou sociální sítě. Zaměříme se na nejpoužívanější z nich a tím je Facebook. Ten podle aktuálních statistik má registrováno přes 1,35 miliardy uživatelů[10]. Vše, co vložíme na náš Facebookový profil, se může stát veřejnou informací. Jméno, věk, pohlaví, každý náš komentář, vložený obsah (obrázky, fotky, dokumenty, videa nebo odkazy), názory, informace o tom, kde jsme a co děláme, kde pracujeme, to vše si může zobrazit téměř kdokoliv (s ohledem na nastavená práva)[11]. Agentura AFP[12] uvedla, že podle odborné studie Tlačítko „To se mi líbí" na Facebooku může o člověku odhalit víc, než sám tuší. Zmíněná studie zjistila, že vzorce sestavené podle Facebookových preferencí jsou schopné poskytnout překvapivě přesné odhady uživatelovy rasy, věku, IQ, sexuální orientace a dalších osobních údajů[13].

Dále sem můžeme zahrnout komentáře na veřejných portálech, námi vytvořené webové stránky nebo členství ve skupinách, které na své stránky umísťují jména členů.

3.1.2 S omezeným přístupem

Do této kategorie můžeme opět zařadit Google i sociální sítě s tím rozdílem, že k získání podrobnějších dat, potřebujeme mít vyšší oprávnění. Tím je myšleno, s kým sdílíme naše data nebo co je zapotřebí k jejich získání. Pokud se zaměříme na Facebook, tak některé informace jsou veřejné a nejde to změnit. U většiny však můžeme nastavit, že

---

[9] Co o vás ví Google? Udělejte si test. *Česká televize* [online]. 1996, 11. 12. 2014 [cit. 2016-01-18]. Dostupné z: http://www.ceskatelevize.cz/ct24/media/1005445-co-o-vas-vi-google-udelejte-si-test

[10] BENNETT, Shea. The 10 Biggest Social Networks Worldwide. *Adweek* [online]. 1978, 24.12.2014 [cit. 2016-01-18]. ISSN 0199-2864. Dostupné z: http://www.adweek.com/socialtimes/largest-social-networks-worldwide/504044

[11] Facebook toho o vás ví mnohem víc, než si myslíte. *Eurozpravy.cz* [online]. 2009, 03. dubna 2015 [cit. 2016-01-18]. ISSN 2336-257X. Dostupné z: http://veda-a-technika.eurozpravy.cz/internet/117195-facebook-toho-o-vas-vi-mnohem-vic-nez-si-myslite

[12] AFP - Agence France-Presse neboli *Francouzská tisková agentura*

[13] Facebook jako špion: prozradí o vás úplně všechno. *Prima Zoom* [online]. 1993 [cit. 2016-01-18]. Dostupné z: http://zoom.iprima.cz/clanky/facebook-jako-spion-prozradi-o-vas-uplne-vsechno

určité informace budou viditelné například pouze pro přátele nebo přátele přátel. Z tohoto důvodu je můžeme označit za data s omezeným přístupem.

Avšak, jak ukazuje experiment s názvem „Neexistuju, ale mám 120 přátel na Facebooku“[14], lehce se mohou i tato data stát veřejnými.

3.1.3 Zcela skryté

Tento druh digitálních stop můžeme považovat za skrytý z toho důvodu, že nejsou v podobě lehce čitelného textu, jako například komentář na sociální síti nebo jako výsledek vyhledávání webového vyhledávače. Jedná se o data, která se shromažďují v podobě souborů, záznamů nebo třeba logů.

3.1.3.1 Cookies

Cookies, neboli textové soubory, které server umísťuje do počítače uživatele webových stránek a které následně odesílají informace o jeho chování zpět na příslušný server, slouží především k zapamatování některých voleb. Díky nim tak například při opakované návštěvě webové stránky nemusíte znovu zaškrtávat požadované položky, nastavovat styl zobrazení apod. Má to ovšem i svou stinnou stranu. Soubory cookies mohou být vytvořeny právě navštívenou stránkou a server si do nich může uložit prakticky cokoliv. Avšak není sám, cookies mohou být vytvořeny také reklamními bannery[15] na aktuální stránce. Mohou si tak o nás shromažďovat nejrůznější informace, které následně mohou zneužít například pro marketing či cílenou reklamu[16].

---

[14] ČIČÁK, Matěj. Experiment: Neexistuju, ale mám 120 přátel na Facebooku. *Zive* [online]. 2007, 20. května 2013 [cit. 2016-01-18]. ISSN 1212-8554. Dostupné z: http://www.zive.cz/clanky/experiment-neexistuju-ale-mam-120-pratel-na-facebooku/priprava-ziskavani-pratel-vetrech-krocich/sc-3-a-168802-ch-86730/default.aspx#articleStart

[15] Banner neboli reklamní proužek (místo pro reklamu)

[16] HNÁT, Ondřej. Uživatel, cookie, sledování a remarketing – kde jsou hranice? *Sunitka* [online]. 2010, 24. prosince 2013 [cit. 2016-01-19]. Dostupné z: http://www.sunitka.cz/c/632-uzivatel-cookie-sledovani-a-remarketing-kde-jsou-hranice

3.1.3.2 Logy na webovém serveru

Log (též žurnál) je název pro záznam nebo soubor záznamů (často textové soubory s příponou: „log“), které si některé programy vytvářejí pro ukládání informací o své činnosti a běhu[17]. V případě serverových logů tyto logy vytváří webový server na základě požadavků, které na něj od uživatelů přicházejí.

Tyto logy mohou obsahovat (v závislosti na nastavení serveru) čas a datum požadovaného dotazu, IP adresu (ze které se dá zjistit lokace odesílatele), konkrétní dotaz či požadavek na server, tedy na jaký odkaz bylo kliknuto, jakou stránku či odpověď požadujeme, otisk prohlížeče (jaký prohlížeč používáme) a také se dá dopočítat čas, strávený na jednotlivých stránkách[18]. Ovšem server logy nejsou tak snadno dostupné a z pravidla k nim má přístup pouze majitel web serveru, případně správce webových stránek[19].

---

[17] Log (log file). *Whatis.com* [online]. 1999 [cit. 2016-01-20]. Dostupné z: http://whatis.techtarget.com/definition/log-log-file

[18] CHRISTENSSON, Per. Digital Footprint. *Techterms* [online]. 2005, May 26, 2014 [cit. 2016-01-20]. Dostupné z: http://techterms.com/definition/digital_footprint

[19] JANOVSKÝ, Dušan. Logy ze serveru. *Jakpsátweb* [online]. 1998 [cit. 2016-01-20]. ISSN 1801-0458. Dostupné z: http://www.jakpsatweb.cz/seo/logy.html

3.2 Možnosti využití a zneužití digitálních stop

Jak využít nebo zneužít digitální stopy je jistě nespočet, zaměříme se však pouze na tu část, která je s digitální stopou spojována nejvíce a to na využití v oblasti kriminalistiky a forenzních vědách, pro potřeby personalistiky, zneužití s cílem krádeže identity a pro potřeby sledování.

3.2.1 Forenzní vědy

Forenzní věda (nebo zkráceně forenzika, forensics), je vědní obor, který se zabývá vyšetřováním, získáváním a (soudním) dokazováním nějakého bezpečnostního incidentu nebo porušení práva státu či pravidel organizace[20]. Cílem digitální forenzní vědy je získání dalších důkazů, které pomohou při vyšetřování široké škály kybernetické kriminality nebo v občanskoprávním řízení. Důkazy z digitálních forenzních vyšetřování obvykle podléhají stejným postupům jako jakékoliv jiné digitální důkazy. Digitální forenzika byla již využita ve spoustě známých procesů a stává se široce přijímaná jako spolehlivá ve Spojených státech i v evropských soudních systémech[21]. Přesto o využití digitálních stop v oblasti forenzní vědy panuje velmi nízké povědomí mezi širokou veřejností, tak i IT odborníky.

3.2.2 Využití pro potřeby personalistiky

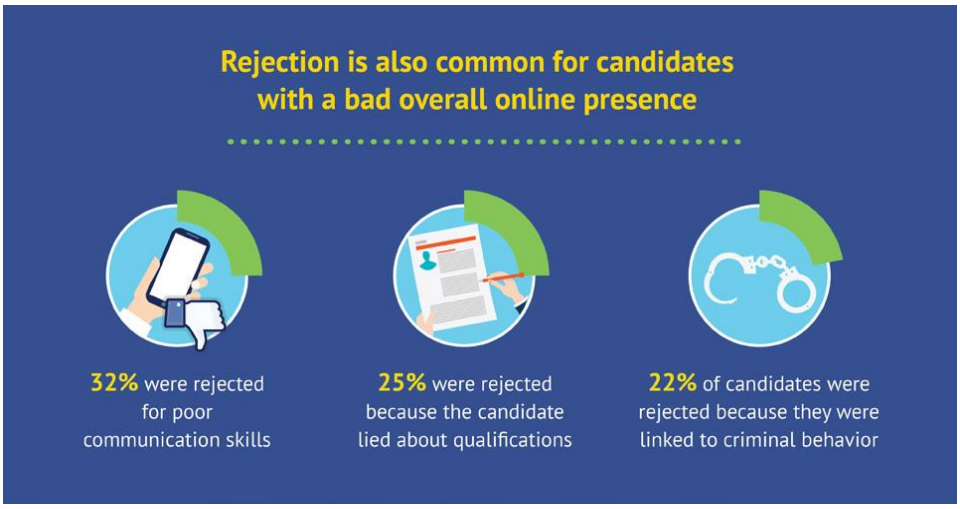
S nástupem sociálních sítí přichází i nový a poměrně jednoduchý způsob, jak získávat osobní i jiné informace o osobě, která nás zajímá. Tento způsob získávání a ověřování informací hojně využívají především personalisté. Uživatele o sobě zanechávají na sociálních sítích velké množství komentářů, názorů, fotek a videí, zveřejňují své zájmy nebo se hlásí k různým skupinám. Personalisté pak tato data sbírají a analyzují. Porovnávají tak například životopis případného uchazeče s informacemi na sociální síti, mohou se také zajímat o jeho komunikační schopnosti, názory na předchozí zaměstnání či

[20] Forenzní věda (Forenzika). *Management Mania* [online]. 2011, 10.05.2013 [cit. 2016-01-21]. Dostupné z: https://managementmania.com/cs/forenzni-veda-forenzika-forensics

[21] KRUSE, Warren G a Jay G HEISER. *Computer forensics: incident response essentials*. Boston, MA: Addison-Wesley, 2001, xiii, 392. ISBN 0201707195.

spolupracovníky, rozsah znalostí či analyzovat vzorce chování. Tato data pak pomáhají personalistům se rozhodnout, zda případného kandidáta o zaměstnání přijmou či zamítnou.

V jakém množství využívají personalisté sociální sítě, ukazuje studie[22], kterou provedla společnost AKKEN Cloud v roce 2015. Zaměřili se na sociální síť Facebook a z výsledků je patrné, že například 46% uchazečů bylo zamítnuto z důvodu provokativních nebo nevhodných fotografií, 28% uchazečů neprošlo přijímacím řízením, protože zveřejnili komentáře s diskriminačním obsahem, 25% uchazečů bylo zamítnuto z důvodu lživých informací uvedených v životopise nebo 32% bylo zamítnuto z důvodu špatné komunikační schopnosti. To ovšem neznamená, že využívání sociálních sítí personalisty má pouze negativní vliv. Například 36% uchazečů bylo označeno za kreativní, což mělo pozitivní vliv na rozhodnutí o přijetí.



Obrázek 2 – výsledky studie
Zdroj: http://www.akkencloud.com/recruiting-on-facebook/

3.2.3 Krádež identity

Za krádež identity se považuje podvodné jednání, kdy se někdo vydává za druhého člověka, s cílem získat finanční prostředky, důležité informace nebo jiné výhody. Pokud pachatel získá naše osobní údaje, což podle zákona č. 101/2000 Sb., o ochraně osobních

[22] WALLACE, Mark. Recruiting on Facebook: How to Ethically Screen Candidates. *Akken Cloud* [online]. 12. 08. 2015 [cit. 2016-01-21]. Dostupné z: http://www.akkencloud.com/recruiting-on-facebook/

údajů[23] jsou: „*jakékoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu*“, můžeme velmi rychle přijít nejen o peníze na svém účtu, ale i zodpovídat za nezaplacené výdaje, za různé škody, dokonce i nést důsledky mnoha trestných činů, které sice spáchala cizí osoba, ale naším jménem[24]. Z pohledu práva je krádež identity považována za dvoustupňový trestný čin.

- Prvním stupněm je získání cizí identity označované jako identity theft.
- Druhým stupněm je následné použití získané identity označované jako identity fraud.

Za citlivé informace, které by mohly podvodníky zajímat, můžeme považovat nejen jméno a příjmení, rodná čísla a čísla osobních dokladů, ale veškeré údaje, podle kterých je možno naši osobu určit, tedy i čísla, PIN a bezpečnostní kódy kreditních karet, adresa bydliště, rodinné či pracovní poměry, detaily o hypotékách a úvěrech apod.[25]

Důvodem pro krádež identity je hned několik. Největší nebezpečí představuje krádež identity pro finanční podvody. Pachatel si tak může pronajmout v půjčovnách auta, která zpětně už nevrátí, nakupovat zbraně, objednávat si hotelové pokoje a za své služby neplatit nebo třeba uzavírat různé smlouvy. Dalším důvodem může být krádež identity s důvodu páchání kriminální činnosti, kdy se pachatel vydává za jinou osobu a orgánům činným v trestním řízení poskytne místo vlastních údajů, údaje odcizené. Jedním z dalších důvodů krádeže identity může být snaha o pošpinění naší pověsti. Pokud si pachatel založí účet na sociální síti pod naším jménem, může tak šířit například extremistické názory nebo

---

[23] Česko. Zákon ze dne 4. dubna 2000 o ochraně osobních údajů a o změně některých zákonů. In: *Sbírka zákonů České republiky*. 2000. Dostupné z: http://www.uoou.cz/files/101_cz.pdf

[24] Ztráta identity. *Policie České republiky* [online]. 2015 [cit. 2016-01-21]. Dostupné z: http://www.policie.cz/clanek/ztrata-identity.aspx

[25] Krádež identity a jak se jí bránit. *Bezpečný internet.cz* [online]. [cit. 2016-01-21]. Dostupné z: http://www.bezpecnyinternet.cz/pokrocily/ochrana-prav/kradez-identity.aspx

propagovat rasovou nesnášenlivost. V některých případech je krádež identity využita za účelem vytvořit si zcela novou identitu a začít život jinde jako nový člověk[26].

3.2.4 Sledování

Možnosti sledování se dají chápat jako monitorování našeho pohybu či polohy. To se však, s výjimkou určení polohy pomocí IP adresy, týká především mobilních zařízení nebo například sledování pomocí veřejných a dopravních kamer. Což ale není předmětem této práce a proto se zaměříme na sledování uživatelů pomocí digitálních stop. Jedná se především o sledování každodenního stereotypu, našich návyků, toho co máme rádi nebo třeba kam často chodíme. Těchto informací se dá zneužít hned několika způsoby. Vynecháme možnosti využití pro potřeby personalistiky, což je popsáno výše, ale zaměříme se na ty ostatní.

Jednou z těch nejčastějších možností je zneužití pro potřeby marketingu a cílené reklamy. Jak již bylo uvedeno, stránky mohou obsahovat logy, reklamní bannery či jiné způsoby sběru a ukládání dat. Ty jsou pak dále zpracovány a nejčastěji prodávány reklamním společnostem, které je používají pro efektivnější a cílenou reklamu. Tím se naše osobní data stávají velmi ceněnou komoditou, označovanou také jako digitální zlato[27]. Časopis Bankovnictví dokonce zveřejnil rozsáhlý článek[28] o tom, jak využít digitální stopu ve prospěch banky. Jako dobrým příkladem zneužití těchto dat je následující úryvek z právě tohoto článku: „*Informace o zájmech a preferencích našeho klienta můžeme využít i v momentě, kdy mu chceme nabídnout bonusové služby, věrnostní program nebo personalizované poradenství. Skutečné řízení vztahů s klienty tak může jít za hranice běžných marketingových nabídek.*“.

---

[26] Ztráta identity. *Policie České republiky*, ref. 24.

[27] STRNAD, Zdeněk. Zmizet není snadné, ale jde to. *E15* [online]. 2007, 23.3.2015 [cit. 2016-01-20]. ISSN 1210-1168. Dostupné z: http://zen.e15.cz/telegraf/zmizet-neni-snadne-ale-jde-to-1169387

[28] Digitální stopa. Máme ji!. *Bankovnictví* [online]. 26. Květen 2015 [cit. 2016-01-20]. ISSN 1214-9810. Dostupné z: http://www.bankovnictvionline.cz/banky-finance/digitalni-stopa-mame-ji

4 Syntetická část

4.1 Kontrola rozsahu vlastní digitální stopy

Každý, kdo někdy používal digitální technologie, zanechával za sebou také určitou digitální stopu. Málo kdo si dokáže představit, kolik se za tu dobu o nás nahromadilo dat a kolik z těchto dat je dohledatelných a potencionálně nebezpečných. Existuje však několik možností, jak prohledat internet a pokusit se tak dohledat vlastní digitální stopy pomocí volně dostupných nástrojů. Uděláme si tak určitou kontrolu rozsahu vlastní digitální stopy a na základě výsledků vyhledávání můžeme udělat dodatečná opatření, ke snížení či úplnému odstranění nalezené digitální stopy.

4.1.1 Běžné vyhledávací možnosti

Jednou ze základních možností, jak vyhledávat digitální stopu, je využití internetového vyhledávače. Pro rozšíření výsledků vyhledávání, můžeme zadat kromě jména, také přezdívky, emaily nebo třeba školy a zároveň použít větší škálu internetových vyhledávačů (Google, Yahoo, Bing, Seznam a jiné). Je nutné si ale uvědomit, že běžné internetové vyhledávače mohou prohledat jen malou část webu, která je označována za povrchový web. Jeho velikost je odhadována asi na 4%[29] celkového obsahu webu[30]. Zbytek obsahu je označován za hluboký web (také známý jako neviditelný nebo skrytý web)[31]. Výsledkem vyhledávání je seznam hypertextových odkazů, který není nijak roztřízený a další zpracování může být poměrně náročné.

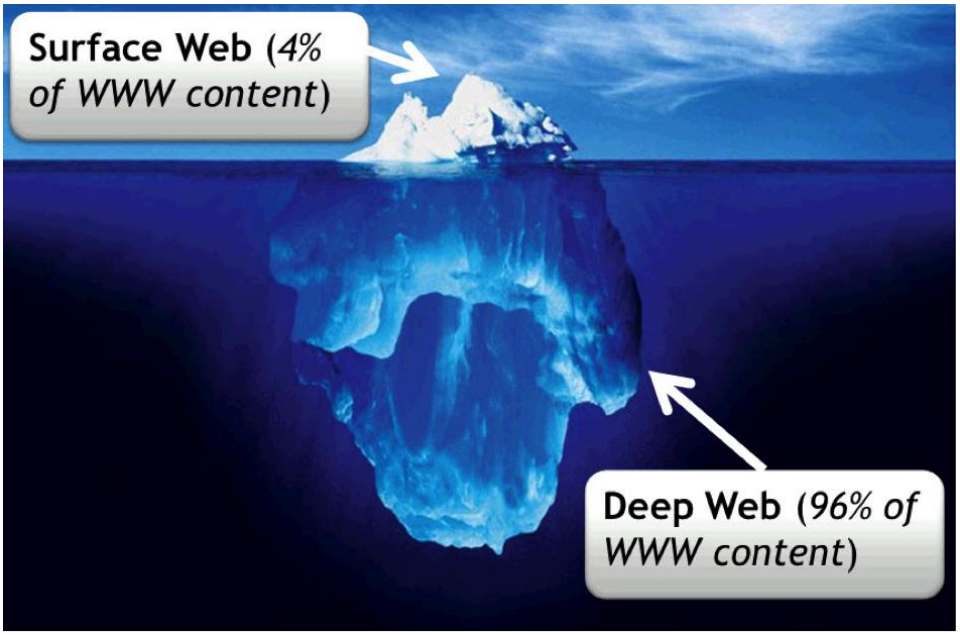
---

[29] YALE, Brad. How the Internet Works: The Deep Web. *InformIt* [online]. 21 října 2014 [cit. 2016-03-07]. Dostupné z: http://www.informit.com/blogs/blog.aspx?uk=How-the-Internet-Works-The-Deep-Web

[30] Překážkou mohou být například formuláře, omezení přístupu ze strany vlastníka, dynamicky generované stránky či zvláštní formáty dokumentů.

TKAČÍKOVÁ, Daniela. Neviditelný web. In: *KTD: Česká terminologická databáze knihovnictví a informační vědy (TDKIV)* [online]. Praha: Národní knihovna ČR, 2014 [cit. 2016-01-22]. Dostupné z: http://aleph.nkp.cz/F/?func=direct&doc_number=000000547&local_base=KTD

[31] The Ultimate Guide to the Invisible Web. In: *Open Education Database (OEDb)* [online]. 2006, 11. 11. 2013 [cit. 2016-01-22]. Dostupné z: http://oedb.org/ilibrarian/invisible-web



Obrázek 3 - Povrchový a hluboký web
Zdroj: http://labs.sogeti.com/category/the-web/page/3

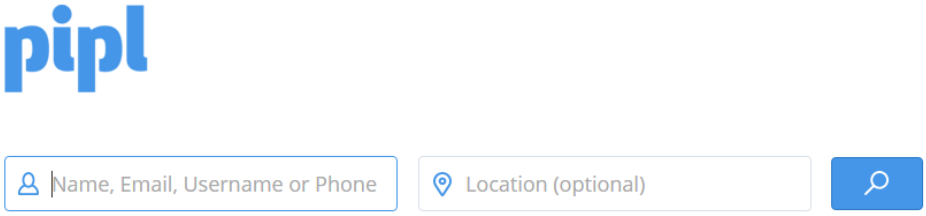
4.1.2 People search engines

Na rozdíl od běžného vyhledávání, můžeme využít tzv. peaople search engines, tedy nástroje, navržené přímo pro hledání lidí na internetu. Hlavním rozdílem a výhodou je přehledné zobrazení výsledků vyhledávání. Výsledky jsou zobrazeny a roztřízeny do jednotlivých kategorií, seskupeny například podle zdroje nalezených dat. Tedy například jedna skupina tvoří data, nalezená na sociálních sítích, další skupina podle shody v emailové adrese nebo třeba podle veřejných záznamů. U každého nalezeného záznamu je pak možné zobrazit další detaily nebo přejít na zdroje těchto dat. Další výhodou vyhledávacích nástrojů je možnost prohledávat i hluboký web. Aktuální objem hlubokého webu je nemožné zjistit, ale odhaduje se, že je zhruba 500x větší, než povrchový web[32]. Nevýhodou však může být, že některé vyhledávací nástroje si za své služby nechají platit.

[32] The Ultimate Guide to the Invisible Web, ref. 30.

4.1.2.1 Pipl

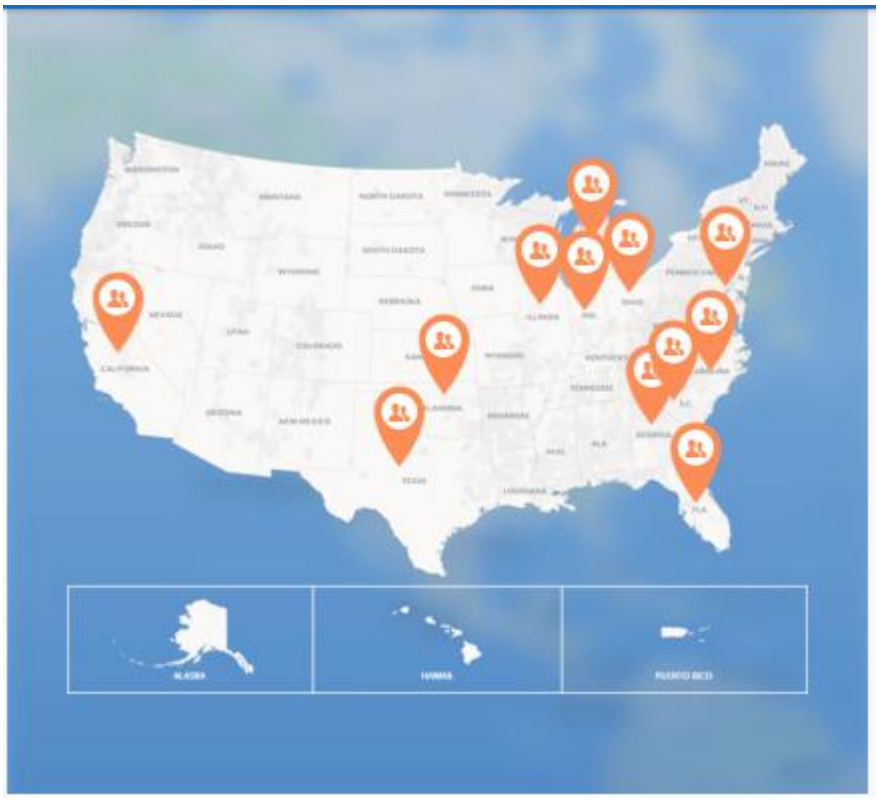
Pipl je jedním z vyhledávacích nástrojů, které umožňují prohledávat i hluboký web. Mezi parametry, podle kterých je možné vyhledávat, patří: jméno, email, telefon, přezdívka a adresa. Výsledky se zobrazují v přehledném seznamu a tento seznam je možné dále filtrovat. Další výhodou je automatické odstranění duplicitních záznamů.



Obrázek 4 – Pipl
Zdroj: https://pipl.com/

4.1.2.2 Spokeo

Tento vyhledávací nástroj také dokáže prohledávat povrchový i hluboký web. Spokeo nabízí vyhledávání podle jména, emailu, telefonu nebo adresy. Výsledkem vyhledávání je kromě přehledného seznamu také mapa, zobrazující pozici nalezených lidí s možností dalšího filtrování.

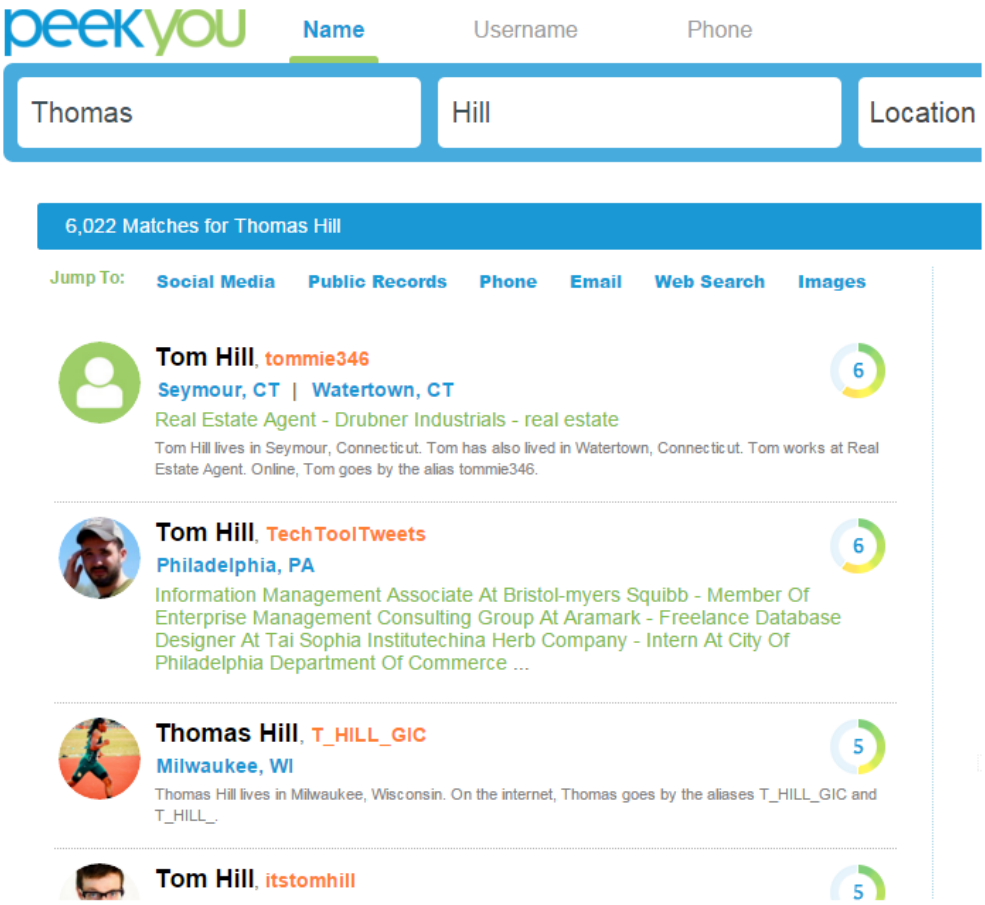


Obrázek 5 – Spokeo mapa
Zdroj: http://www.spokeo.com/

Nevýhodou tohoto nástroje je, že vyhledává pouze na území USA.

4.1.2.3 PeekYou

PeekYou je vyhledávací nástroj, který se zaměřuje hlavně na sociální sítě. Vyhledávat se dá podle jména, přezdívky nebo telefonního čísla. Výsledkem vyhledávání se kategorizovaný seznam podle zdroje nalezených dat. Dokáže také prohledávat obsahy dokumentů a zobrazuje i výsledky, které mají alespoň částečnou shodu s hledaným výrazem.



Obrázek 6 – PeekYou

Zdroj: http://www.peekyou.com/

4.1.2.4 Jiné vyhledávače

Mezi další vyhledávací nástroje patří Intelius, PeopleFinders, ZabaSearch nebo například WhitePages.

4.1.3 Možnosti používaných služeb

Některé služby mají integrované nástroje, pro kontrolu rozsahu digitální stopy a možnosti spravování těchto dat. Po přihlášení do námi využívaných služeb, jako je například Google nebo Facebook, můžeme zobrazit nebo si vyžádat (ve formě souboru) data, která jsou o nás shromažďována.

4.1.3.1 Facebook information

Sociální síť Facebook nabízí svým uživatelům dvě možnosti, které mohou využít, při kontrole dat. První možností je zobrazení záznamů o aktivitách, která obsahuje seznam všech příspěvků a činností od založení účtu[33]. Druhou možností je stáhnout soubor se svými daty. Přestože by se mohlo zdát, že jde o užitečný nástroj, který umožní uživateli stáhnout kompletní data, která o uživateli Facebook nashromáždil, není tomu tak. Ve skutečnosti tak uživatel stáhne pouze kopii profilu, což je zhruba 29% všech našich dat, uchovávaných společností Facebook. Pro získání veškerých dat, musí uživatel zaslat písemnou žádost přímo společnosti Facebook[34].

4.1.3.2 Google dashboard

Google dashboard neboli hlavní panel Googlu dává k dispozici několik různých nástrojů, které pomáhají uživateli spravovat jeho soukromí. Uživatel tak může přehledně zjistit, jaká data a v jaké míře jsou o něm shromažďována a případně upravit nastavení, ovlivňující sběr dat a zobrazování reklam. Některé nastavení vyžaduje přihlášení uživatele, což však zahrnuje rozšířené možnosti kontroly dat a nastavení napříč všemi aplikacemi, které Google nabízí[35].

---

[33] Prozkoumejte své záznamy o aktivitách. *Facebook* [online]. 2010 [cit. 2016-01-23]. Dostupné z: https://www.facebook.com/help/437430672945092

[34] Get your Data!. *Europe versus Facebook* [online]. Austria, 2012 [cit. 2016-01-24]. Dostupné z: http://europe-v-facebook.org/EN/Get_your_Data_/get_your_data_.html

[35] Zobrazení dat a aktivity na účtu na Hlavním panelu Google. *Google* [online]. 1998 [cit. 2016-01-24]. Dostupné z: https://support.google.com/accounts/answer/162744?hl=cs

4.2 Odstranění a správa digitální stopy

Rozhodně nejlepším způsobem, jak zabránit tvorbě a zneužívání digitálních stop je, nepoužívat digitální technologie. To si ale v dnešní době umí představit jen málokdo a v mnoha případech to ani není možné. Z toho vyplívá, že zanechávání digitální stopy se nevyhneme.

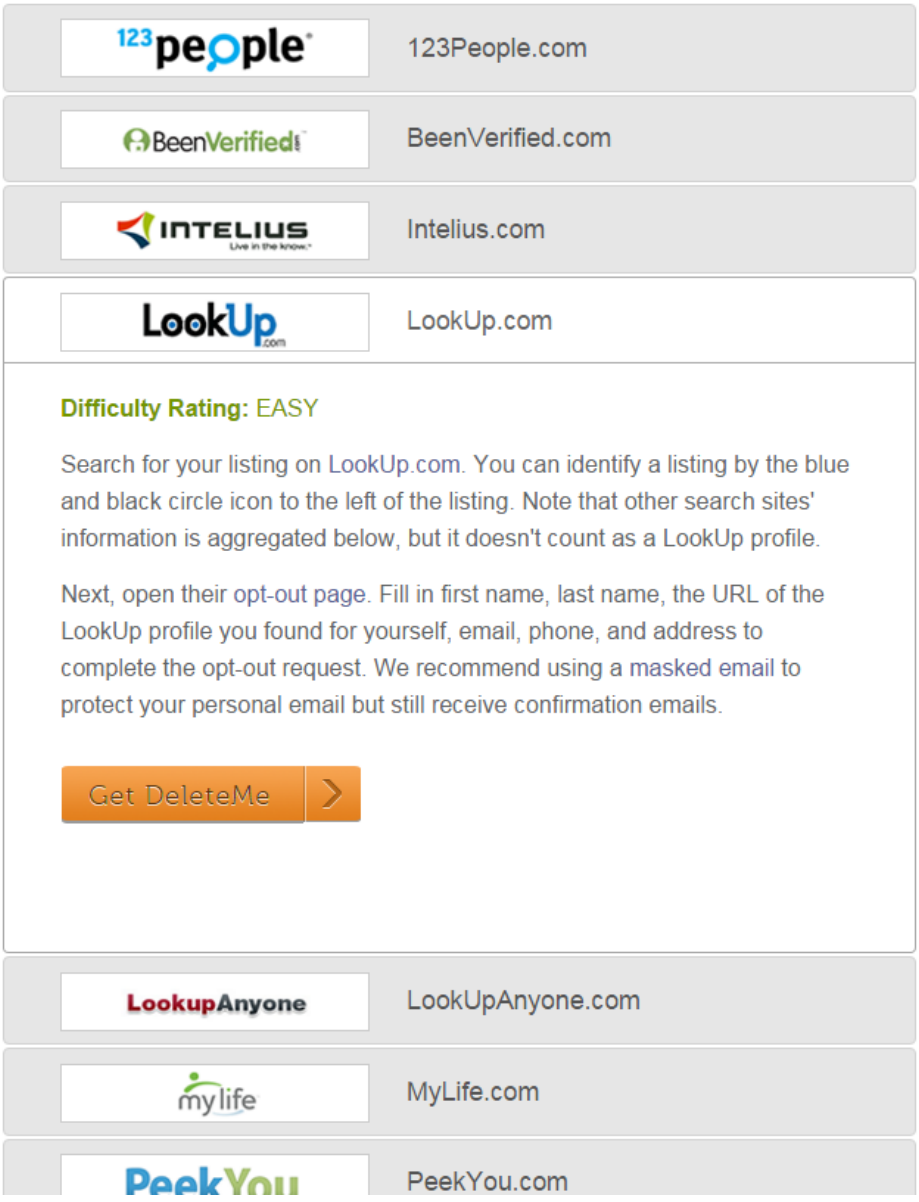
4.2.1 Odstranění stop v prostředí internetu

Po zjištění rozsahu vlastní digitální stopy se můžeme pokusit o smazání těchto stop. K dispozici máme několik možností, počínaje mazáním obsahu vlastních stránek a blogů, přes mazání obsahu, účtu a uložených dat na straně poskytovatele služeb, jako jsou například sociální sítě, mailové služby a jiné nebo můžeme využít některých sofistikovaných nástrojů, určených právě pro tento účel. Existují i firmy, které se zabývají úpravou či mazáním naší digitální stopy, především za účelem lepší veřejné reputace. Avšak podle společnosti ReputationDefender, zabývající se již několik let změnou a mazáním digitální stopy, je v dnešní době nemožné, upravit či smazat vše, co je o nás na internetu uloženo. Upravitelný obsah se podle ReputationDefender pohybuje okolo 80 – 90% v závislosti na čase a financích, které jsem do toho ochotni investovat[36].

Nejjednodušší částí mazání vlastní digitální stopy je odstranit data z vlastních webových stránek či blogů. O něco málo složitější, ale stále ještě triviální, je smazání sledovacích souboru, uložených v počítači. Přestože se tyto soubory dají vymazat ručně, je značně pohodlnější a mnohdy spolehlivější použít nástroj k tomu určený. Tento způsob a nástroje jsou popsány níže. Další stupněm mazání digitální stopy je odstranění výsledků vyhledávání z již výše zmiňovaných People Search Engine. Online soukromá společnost Albine, zabývající se kontrolou osobních informací na internetu, vydala nástroj zvaný DeleteMe, určený na mazání a kontrolu informací, které jsou dohledatelné pomocí People

[36] MARTÍNEZ-CABRERA, Alejandro. Erasing all digital footprints 'impossible'. *San Francisco chronicle* [online]. San Francisco, Calif.: Chas. D. Young, July 6, 2010 [cit. 2012-05-14]. ISSN 1932-8672. Dostupné z: http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2010/07/05/BU4V1E8D9V.DTL

Search Engines.[37] Také vydali článek[38], kde si uživatel může najít, jak ručně tato data vymazat na nejrůznějších stránkách vyhledávačů People Search Engine.



Obrázek 7 – Možnosti mazání dat z vyhledávačů People search engines
Zdroj: https://www.abine.com/optouts.php

[37] Delete Your Personal Information From The Internet. *Abine* [online]. 280 Summer St. Boston, 2015 [cit. 2016-02-26]. Dostupné z: https://www.abine.com/deleteme/landing.php

[38] How To Protect Your Data And Remove Personal Information From The Internet. *Abine* [online]. 280 Summer St. Boston, 2015 [cit. 2016-02-26]. Dostupné z: https://www.abine.com/optouts.php

Značně složitější je odstranění osobních informací a dat ze strany nejrůznějších poskytovatelů služeb jako jsou sociální sítě, maily, wikipedie, vyhledávače a jiné. Mnohdy i odstranění samotného účtu je velmi složité a v některých případech dokonce nemožné. Velmi pěkný postup mazání účtu a jeho obtížnost popisuje ve svém článku[39] Cameron Chapman. Například smazání účtu na Facebooku je jedno z nejtěžších a účet na wikipedii se smazat nedá[40].

4.2.2 Odstranění sledovacích souborů´

Za sledovací soubory považujeme především Cookies a existuje hned několik typů těchto potencionálně nebezpečných souborů. Jsou typy cookie, které lze odstranit celkem snadno a zvládne to buď jednoduchý nástroj nebo i webový prohlížeč. Existují ale i další typy jako jsou například Flash Cookie nebo SilverLight Cookie, které již není tak snadné odstranit.[41] Následuje několik vhodných nástrojů, vybraných podle serveru addictivetips[42], které mohou tyto druhy sledovacích souborů vymazat.

4.2.2.1 Webový prohlížeč

Mezi 4 nejpoužívanější prohlížeče internetu patří, podle serveru W3counter[43], Google Chrome, Safari, Internet Explorer a Mozzila Firefox. Každý z těchto webových prohlížečů umožňuje vymazání cookies. Bohužel však to nezahrnuje flash cookie a

---

[39] CHAPMAN, Cameron. How to permanently delete your account on popular websites. *Smashing Magazine* [online]. 2016, June 11th, 2010 [cit. 2016-02-26]. Dostupné z: https://www.smashingmagazine.com/2010/06/how-to-permanently-delete-your-account-on-popular-websites/

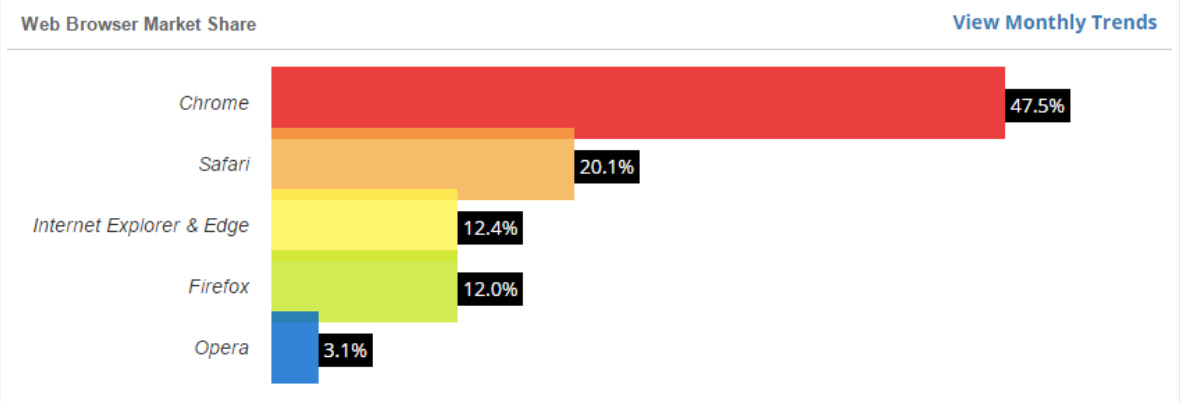
[40] CHAPMAN, Cameron. How to permanently delete your account on popular websites. *Smashing Magazine. Ref. 39*

[41] Different types of Internet Cookies. *The Windows Club* [online]. 2016 [cit. 2016-02-27]. Dostupné z: http://www.thewindowsclub.com/types-of-internet-cookies

[42] FARSHAD. Which System Cleaner To Use? We Compare The Best Cleaning Utilities. *AddictiveTips* [online]. 2016, May 21, 2011 [cit. 2016-02-27]. Dostupné z: http://www.addictivetips.com/windows-tips/which-system-cleaner-to-use-we-compare-the-best-cleaning-utilities/

[43] W3Counter: Global Web Stats - January 2016. *W3Counter* [online]. 2004 - 2016, January 2016 [cit. 2016-02-27]. Dostupné z: http://www.w3counter.com/globalstats.php?year=2016&month=1

silverlight cookie. Jedinou možností, jak tyto speciální typy cookie, bez použití nástrojů třetích stran, je vymazat je ručně, či pomocí operačního systému.[44]



Obrázek 8 – Nejpoužívanější webové prohlížeče

Zdroj: https://www.w3counter.com/globalstats.php?year=2016&month=2

4.2.2.2 Ccleaner

Ccleaner je nástroj pro optimalizaci systému. Odstraňuje nepoužívané soubory ze systému a tím uvolňuje místo na disku. Důležité je, že dokáže odstranit veškerou internetovou historii ze vše nejpoužívanějších internetových prohlížečů a i z mnoha dlaších, včetně cookies a to i flash a silverlight. Mimo jiné nabízí i čištění registrů. Je možné i nastavit, jaké typy souborů se mají zachovat, tedy seznam chráněných souborů, mezi které se dají zařadit například soubory s pamětí nastavení či hesel.[45]

4.2.2.3 IObit Advanced SystemCare

Advanced SystemCare od společnosti IObit nabízí spoustu užitečných funkcí pro správu, údržbu a zrychlení PC. Mezi tyto funkce patří například mazání historie, čištění registrů nebo odstranění nepoužívaných ikon a souborů. Jedou z funkcí je i odstranění dočasných souborů, tedy i cookies a to i flash a silverlight. Odstraňuje i vyplněné formuláře a uložená hesla. Advanced SystemCare umožňuje vytvoření chráněných

---

[44] STOCKLEY, Mark. How to clear out cookies, Flash cookies and local storage. *Naked Security* [online]. 1985, 05 NOV 2014 [cit. 2016-02-27]. Dostupné z: https://nakedsecurity.sophos.com/2014/11/05/how-to-clear-out-cookies-flash-cookies-and-local-storage

[45] Ccleaner - vlastnosti. *Piriform* [online]. 2005 - 2016 [cit. 2016-02-27]. Dostupné z: https://www.piriform.com/ccleaner/features

souborů, které nebudou podléhat mazání nebo testování na přítomnost nežádoucího programu. Umožní tak zachovat cookies, které slouží pouze pro uchování nastavení.[46]

4.2.2.4 Glary Utilities

Glary Untilities je jedním z dlaších možností, jak jednoduše čistit počítač od nežádoucích souborů. Mezi jeho základní funkce patří čištění registrů, defragmentace disku i registrů, mazání nefunkčních ikon nebo například mazání historie procházení. Dokáže promazat všechny zmiňované druhy cookies a obsahuje i možnost chráněných souborů. Má také dvě úrovně ovládání. Pro nezkušené uživatele nabízí možnost vyčištění počítače jedním tlačítkem, bez možnosti nastavení. Pro pokročilejší uživatele je zde možnost nastavit, které soubory zachovat a které smazat. Většina funkcí však není zadarmo.

4.2.3 Nástroje zabraňující sledování

Jak již bylo několikrát uvedeno, během surfování na internetu můžeme být sledováni prostřednictvím například cookies nebo pixelovým tagem. Existuje několik nástrojů, které jsou tzv. doplňkem webového prohlížeče a které nám pomáhají zabránit tomuto sledování. Doplňků je celá řada a proto se zaměříme především na ty, které mají širokou podporu webových prohlížečů a plní funkci zabraňující sledování. Budou nás zajímat hlavně doplňky, fungující na nejpoužívanějších webových prohlížečích, které jsou Google Chrome, Safari, Internet Explorer a Firefox[47]. Z toho důvodu se zaměříme na AdBlock plus, Disconnect a Ghostery.

4.2.3.1 AdBlock plus

AdBlock plus je nástroj zdarma, podporovaný prohlížeči Google Chrome, Safari a Firefox. Tento nástroj blokuje veškeré sledování, reklamy, vyskakovací okna, malware, bannery a video-reklamy i na Facebooku a Youtube. Vedlejším efektem zakázání reklam,

---

[46] Advanced SystemCare 9 User Manual. *IObit* [online]. 2005 - 2016 [cit. 2016-02-27]. Dostupné z: http://www.iobit.com/product-manuals/asc-help

[47] W3Counter: Global Web Stats - January 2016. *W3Counter*. Ref. 42.

je menší objem dat, potřebný k zobrazení a tedy zrychlení surfování po internetu. AdBlock pracuje mnohdy natolik dobře, že již čelil několika soudům ze stran reklamních agentur či poskytovatelů webových stránek, které díky blokování reklam přicházejí o své zisky[48].

Obrázek 9 – AdBlock Plus

AdBlock umožňuje také vložit si libovolnou stránku do seznamu povolených, tzv. whitelist, čímž nebude blokovat reklamy či jiný obsah, například videa, na dané sránce.[49]

4.2.3.2 Disconnect

Disconnect je nástroj, podporovaný prohlížeči Google Chrome, Safari, Internet Explorer a Firefox. Chrání uživatele před sledováním, malwarem, blokuje sledovací

[48] WILLIAMS, Ben. Adblock Plus and (a little) more. *AdBlock Plus* [online]. 2015-05-27 [cit. 2016-02-28]. Dostupné z: https://adblockplus.org/blog/another-court-another-obvious-win-for-ad-blocking-and-acceptable-ads-too

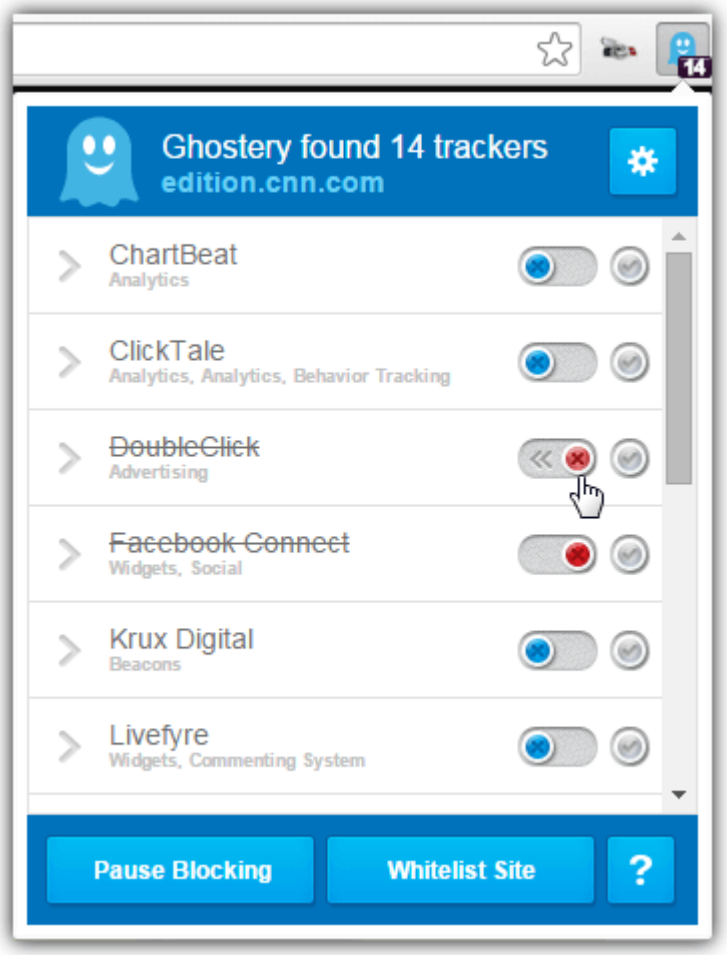
[49] Tutorials. *AdBlock Plus* [online]. [cit. 2016-02-28]. Dostupné z: https://adblockplus.org/en/tutorials

cookies třetích stran s také nabízí zabezpečení WI-FI. Většina těchto funkcí je ale placená, verze zdarma však nabízí ochranu proti sledování, blokování cookies třetích stran a nabízí možnost soukromého vyhledávání.[50]

4.2.3.3 Ghostery

Ghostery je podporované rozšíření pro Google Chrome, Safari, Internet Explorer a Firefox. Tento nástroj aktivně blokuje pokusy o sledování uživatele v podobě sledovacích cookies nebo pixelového tagu. Ghostery v průběhu surfování informuje o aktuálně zablokovaných pokusech o sledování či reklamy na aktuální stránce s možností přehledného výpisu a možností povolení či zakázání daného obsahu.

[50] HENRY, Alan. The Best Browser Extensions that Protect Your Privacy. *Lifehacker* [online]. 2005, 2015-08-31 [cit. 2016-02-28]. Dostupné z: http://lifehacker.com/the-best-browser-extensions-that-protect-your-privacy-479408034



Obrázek 10 – Ghostery

Na rozdíl od ostatních nástrojů, Ghostery v základním nastavení neblokuje vůbec nic, nejdříve poskytne informace o počtu nežádoucích zařízení a společnosti, které patří a poté se uživatel může rozhodnout, zda dané zařízení zablokuje nebo ne. Toto nastavení si pak Ghostery zapamatuje a aplikuje ho na všech následujících webových stránkách.[51]

4.2.4 Nástroje zajišťující anonymitu

Dalším stupněm zvýšení bezpečnosti a ochrany soukromí uživatele je zajištění anonymního surfování na internetu. Běžným surfováním zanecháváme malé střípky stop, které dohromady dají něco, co se dá nazvat jako digitální otisk prstu prohlížeče. Jedná se o data, která prohlížeč odesílá, aby dostal co možná nejoptimálnější obsah (jazyk, rozlišení,

[51] Ghostery. *Jak na webové stránky - Zvyšování výkonu a bezpečnost webových stránek* [online]. 2005, 19.11.2015 [cit. 2016-02-28]. Dostupné z: http://timehosting.cz/ghostery/

verze a typ prohlížeče, operační systém a jiné). Další informace o nás prozrazuje IP adresa nebo některé doplňky či Java a Flash.[52] Míru anonymity tedy určuje schopnost, tyto identifikátory odstranit, změnit či skrýt. K tomuto účelu existuje množství nástrojů, které více či méně zajišťují anonymitu na internetu.

4.2.4.1 Anonymní prohlížení v rámci prohlížeče

Řada internetových prohlížečů nabízí možnost anonymního prohlížení, čímž poskytují jednoduchou formu anonymního surfování. Anonymní režim v prohlížeči pouze zabraňuje uživatelům stejného počítače zobrazení historie procházení a také nejsou ukládány žádné soubory cookies nebo jsou po ukončení relace vymazány. Nedokáží však změnit či skrýt IP adresu, z čehož vyplývá, že vůči internetu nejsme v žádném případě anonymní.

Dalším stupněm jsou webové proxy anonymizéry, které fungují na principu přesměrování. Jedná se o webovou stránku, na kterou vložíme internetový odkaz, ta odešle dotaz s vlastní IP adresou a zobrazí výsledek odkazu. Má to však několik nevýhod. Nevíme úroveň důvěryhodnosti poskytovatele anonymizéru, rychlost odezvy závisí také na poskytovateli anonymizéru.

Obdobně jsou na tom klasické proxy servery, které se nastavují přímo v prohlížeči a fungují jako jakýsi prostředník či uzel, přes který chodí naše dotazy zakryté pod IP adresou poskytovatele serveru.

Nejvyšší možnou úrovní ochrany soukromí jsou služby, fungující na principu kaskádových uzlů. Ty fungují (zjednodušeně řečeno) jako proxy servery zapojené v řadě za sebou, přičemž konkrétní informaci, odkud a kam proudí data, mají jen dva po sobě následující servery. Navíc, pro vyšší bezpečnost, jsou data šifrovaná. V praxi tuto metodu anonymizace využívají sítě JAP/JanDonym a Tor.[53]

---

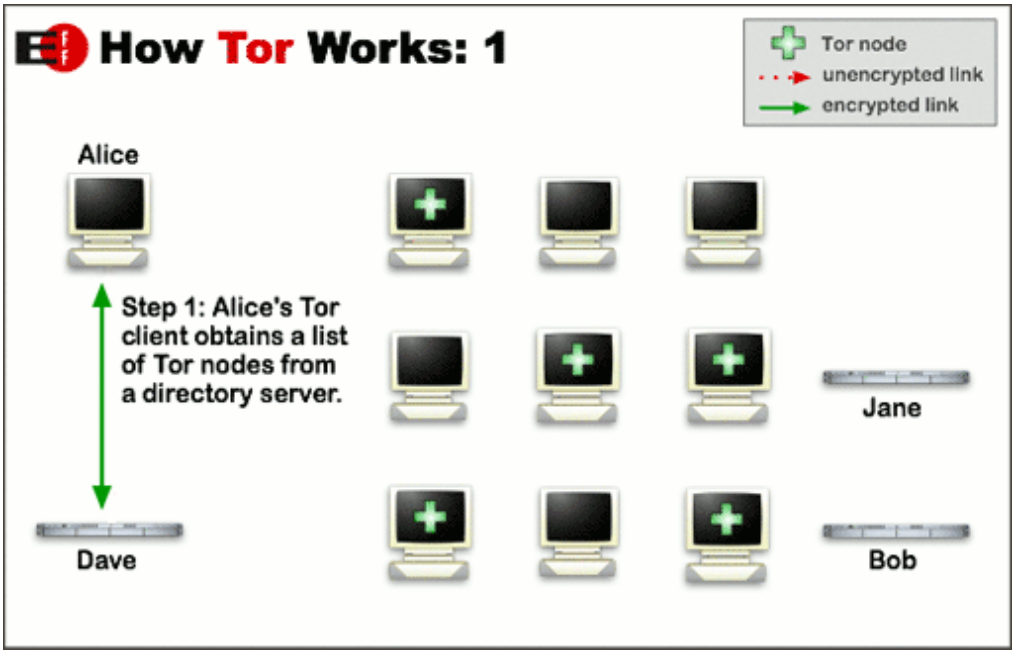
[52] KRATOCHVÍL, Petr. Anonymní surfováni. *Chip* [online]. Německo: CHIP Communications, 2016, 02.07.2013 [cit. 2016-02-28]. ISSN 0170-6632. Dostupné z: http://www.chip.cz/casopis-chip/earchiv/rubriky/technika/anonymni-surfovani

[53] KRATOCHVÍL, Petr. Anonymní surfováni. *Chip* . Ref. 51.

4.2.4.2 Tor

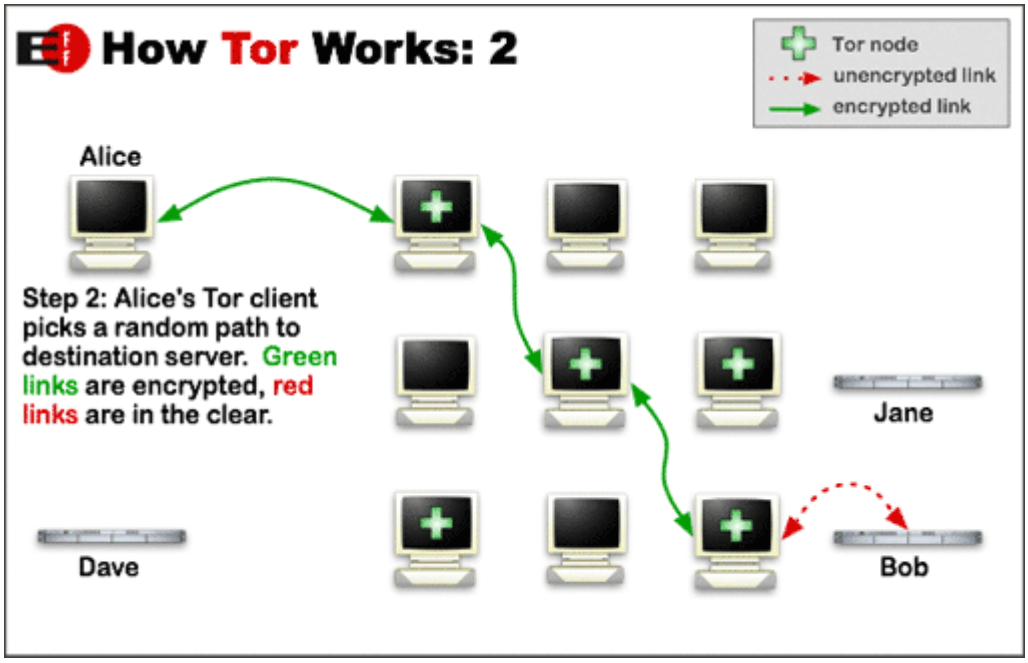
Název Tor vznikl jako zkratka z projektu The Onion Routing (cibulové směrování) který měl zajistit ochranu vládní komunikace. V současné době převzala projekt nezisková organizace The Tor Project, která se skládá převážně z dobrovolníků a dala tuto službu zdarma k dispozici široké veřejnosti.

Při běžné komunikaci klient – server jdou data nešifrovaná a navíc server přesně ví, kdo se ptá, a tedy kam má poslat data zpět. Tor využívá síť routerů, přes který směřuje komunikaci a to způsobem, že router, který obdrží požadavek, zná pouze předchozí a následující router. Neví tedy nic o tom, kdo se ptá a ani jaký je konečný cíl. Navíc data jsou zašifrovaná do vrstev (odtud cibulové směrování), jejichž počet odpovídá počtu routerů, přes které půjde komunikace. Každý router tedy nejprve rozšifruje svou vrstvu, podívá se, kam má směrovat dál a odešle dalšímu. Až úplně poslední rouret v řadě rozbalí požadavek a dotáže se na požadovaný server. Odpověď pak opět zašifruje a pošle zpět na předchozí router. Tak to funguje, až zprávu opět obdrží klient. Šifrování a návrh trasy zřizuje klient na straně uživatele.



Obrázek 11 – Tor

Zdroj: https://www.torproject.org/about/overview.html.en



Obrázek 12 – Tor

Zdroj: https://www.torproject.org/about/overview.html.en

Nevýhodou je extrémně pomalé připojení, které je dáno nejpomalejším prvkem na trase. Vzhledem k tomu, že Tor je nezisková organizace a většina routeru jsou počítače dobrovolníků, nelze očekávat závratnou rychlost.[54] V současnosti existuje zhruba 7000 uzlů, přes které Tor funguje.[55]

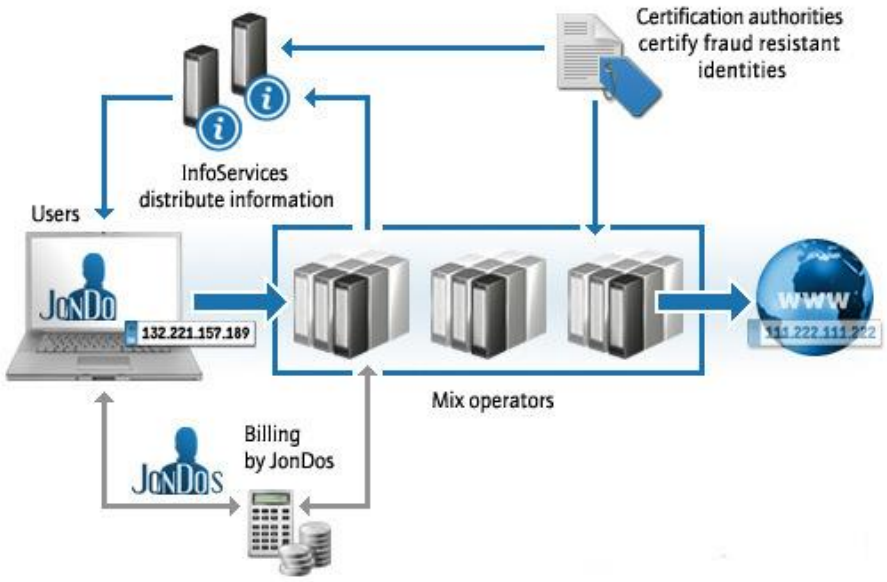
4.2.4.3 JonDonym

JonDonym neboli JAP (Java Anon Proxy) je Javová aplikace, fungující podobně jako Tor. Rozdíl jen, že Jondonym mění IP adresu klienta a po zašifrování pošle dotaz mezi tzv. mix serveru. V Mixech se pohybují data všech aktuálních uživatelů pod stejnou IP adresou prvního proxy serveru, čímž znemožňují identifikovat uživatele. Na rozdíl od Toru, se mix serverem nemůže stát kdokoliv, ale každý musí prokázat svoji identitu u nejméně jedné ze tří stávajících certifikačních autorit, kterými jsou JonDos, AN.ON a German Privacy Foundation. Uživatel si pak může vybrat, přes které mixy pošle svůj

[54] Tor Project: Overview. *Tor Project: Anonymity Online* [online]. 2004 [cit. 2016-02-28]. Dostupné z: https://www.torproject.org/about/overview.html.en

[55] Tor Metrics - Relays with Exit, Fast, Guard, Stable, and HSDir flags. *Tor Metrics* [online]. 2004, 2016-02-28 [cit. 2016-02-28]. Dostupné z: https://metrics.torproject.org/relayflags.html

dotaz. JonDonym se dá využít pomocí aplikace JonDo nebo JonDoFox a to buď verze zdarma nebo placenou, která je zvýhodněna především o vyšší rychlost.[56]



Obrázek 13 – JonDonym

Zdroj: https://anonymous-proxy-servers.net/en/overview.html

[56] JonDo Help: JonDonym. *JonDonym - the anonymisation service* [online]. 2006 [cit. 2016-02-28]. Dostupné z: https://anonymous-proxy-servers.net/en/help/jondonym.html

5 Výsledky a diskuse

5.1 Možnosti kontroly

Vzhledem k možnostem zneužití digitální stopy, popsané v kapitole 3.2, by měl každý uživatel internetu znát rozsah své digitální stopy. V současné době existuje několik možností, které může uživatel využít, aby zjistil, kolik a jakých informací po sobě zanechal.

Za použití internetových vyhledávačů, jako je Google, Yahoo! nebo například Bing, může uživatel prohledat tzv. povrchový web, který tvoří zhruba 4% celkového obsahu webu[57]. Z této části webu, je prohledávána pouze indexovaná část, která tvoří cca 8% z povrchového webu. Například Google indexuje okolo 48 miliard webových stránek, což tvoří 0.03% obsahu celkového webu.[58] K lepší představě o rozsahu vlastní digitální stopy je tedy zapotřebí použít i další nástroje, mezi které patří i People search Engine, popsané v kapitole 4.1.2, schopné prohledat i hluboký web nebo využít možnosti využívaných služeb (například: Facebook information, nebo Google Dashboard), popsané v kapitole 4.1.3.

5.2 Eliminace vlastní digitální stopy

Jakmile má uživatel představu o rozsahu své digitální stopy, může využít některé nástroje, určené k eliminaci digitální stopy a ke zvýšení bezpečnosti a ochrany soukromí uživatele.

Vzhledem k obtížnosti mazání některých druhů sledovacích souborů, jako jsou například Flash a SilverLight cookies, může uživatel využít sofistikovaných nástrojů (Ccleaner, Advanced SystemCare) pro jejich snazší odstranění. K zabránění dalšímu

[57] YALE, Brad. How the Internet Works: The Deep Web. Ref 29.

[58] Total number of Websites & Size of the Internet as of 2013 : Facts Hunt. *Facts Hunt* [online]. 2016 [cit. 2016-03-07]. Dostupné z: http://www.factshunt.com/2014/01/total-number-of-websites-size-of.html

sledování uživatele je možné využít například AdBlock Plus, Disconnect nebo Ghostery, kteří aktivně blokují sledovací nástroje třetích stran. Některé webové stránky obsahují nemálo těchto tzv. trackerů. Například Googleanalytics.com obsahuje 87 trackerů, youtube.com - 68, facebook.com - 27, zive.cz - 7 nebo svethardware.cz - 6 trackerů.[59]

Další stupněm ochrany soukromí uživatelů je mazání digitální stopy na internetu. Některá data z internetu může odstranit sám uživatel. Jedná se především o data na vlastních webových stránkách. Dále je doporučen nástroj DeleteMe, určený na mazání a kontrolu informací, které jsou dohledatelné pomocí People Search Engines. Další možností je využití funkcí Google Dashboard, díky které může uživatel spravovat data, získaná společností Google. V rámci zvýšení bezpečnosti se může uživatel pokusit také smazat kompletní profily založené na stránkách jako je například: Facebook, Google, Twitter nebo třeba eBay. Zde se však může setkat s nečekaným odporem, který je daný tím, že většina těchto společností profituje z počtu uživatelů. Například pokud uživatel zažádá o smazání účtu na Facebooku, bude účet smazán nejdřív 14 dní po zadání žádosti za předpokladu, že se nikdo během této doby na účet nepřihlásí, jinak bude žádost zrušena. Na Wikipedii se dokonce účet nedá smazat vůbec.[60]

Podle společnosti ReputationDefender, zabývající se již několik let změnou a mazáním digitální stopy, je v dnešní době nemožné, upravit či smazat vše, co je o uživateli na internetu uloženo. Upravitelný obsah se podle ReputationDefender pohybuje okolo 80 – 90%.[61]

---

[59] V síti datových dealerů. *Chip* [online]. 1978, **2013**(04) [cit. 2016-03-07]. ISSN 0170-6632. Dostupné z: http://www.chip.cz/casopis-chip/earchiv/vydani/rocnik-2013/chip-04-2013/v-siti-dat/

[60] CHAPMAN, Cameron. How to permanently delete your account on popular websites. *Smashing Magazine. Ref. 39*

[61] MARTÍNEZ-CABRERA, Alejandro. Erasing all digital footprints 'impossible'. Ref. 36.

6 Závěr

Vzhledem k možnostem využití či zneužití digitální stopy, byly navrženy nástroje, které pomohou uživateli kontrolovat její rozsah (People search engines, Google Dashboard, Facebook information) a na základě těchto informací spravovat či eliminovat vzniklou digitální stopu (DeleteMe, Google Dashboard). Dále byly navrženy nástroje pro zabránění dalšímu sledování uživatele (AdBlock Plus, Disconnect, Ghostery) a vymazání již uložených sledovacích souborů (Ccleaner, Advanced SystemCare, Glary Utilities).

Pro zajištění anonymity uživatele a zvýšení tak ochrany soukromí, jsou k dispozici anonymizační sítě Tor a JanDonym. Při použití těchto sítí musí však uživatel počítat s velmi nízkou rychlostí a omezenou propustností dat.

Z výsledků analýzy hrozeb, možností kontroly a odstranění digitální stopy vyplývá, že není v silách uživatele odstranit veškeré stopy, které vznikají při používání internetu. Je však schopen pomocí různých nástrojů tuto stopu minimalizovat a tím snížit rizika, spojená s digitální stopou.

7 Použitá literatura a zdroje

Advanced SystemCare 9 User Manual. *IObit* [online]. 2005 - 2016 [cit. 2016-02-27]. Dostupné z: http://www.iobit.com/product-manuals/asc-help

BENNETT, Shea. The 10 Biggest Social Networks Worldwide. *Adweek* [online]. 1978, 24.12.2014 [cit. 2016-01-18]. ISSN 0199-2864. Dostupné z: http://www.adweek.com/socialtimes/largest-social-networks-worldwide/504044

Ccleaner - vlastnosti. *Piriform* [online]. 2016 [cit. 2016-02-27]. Dostupné z: https://www.piriform.com/ccleaner/features

Co o vás ví Google? Udělejte si test. *Česká televize* [online]. 1996, 11. 12. 2014 [cit. 2016-01-18]. Dostupné z: http://www.ceskatelevize.cz/ct24/media/1005445-co-o-vas-vi-google-udelejte-si-test

Česko. Zákon ze dne 4. dubna 2000 o ochraně osobních údajů a o změně některých zákonů. In: *Sbírka zákonů České republiky*. 2000. Dostupné z: http://www.uoou.cz/files/101_cz.pdf

ČIČÁK, Matěj. Experiment: Neexistuju, ale mám 120 přátel na Facebooku. *Zive* [online]. 2007, 20. května 2013 [cit. 2016-01-18]. ISSN 1212-8554. Dostupné z: http://www.zive.cz/clanky/experiment-neexistuju-ale-mam-120-pratel-na-facebooku/priprava-ziskavani-pratel-vetrech-krocich/sc-3-a-168802-ch-86730/default.aspx#articleStart

Delete Your Personal Information From The Internet. *Abine* [online]. 280 Summer St. Boston, 2015 [cit. 2016-02-26]. Dostupné z: https://www.abine.com/deleteme/landing.php

Different types of Internet Cookies. *The Windows Club* [online]. 2016 [cit. 2016-02-27]. Dostupné z: http://www.thewindowsclub.com/types-of-internet-cookies

Digitální stopa. Máme ji!. *Bankovnictví* [online]. 26. Květen 2015 [cit. 2016-01-20]. ISSN 1214-9810. Dostupné z: http://www.bankovnictvionline.cz/banky-finance/digitalni-stopa-mame-ji

Facebook jako špion: prozradí o vás úplně všechno. *Prima Zoom* [online]. 1993 [cit. 2016-01-18]. Dostupné z: http://zoom.iprima.cz/clanky/facebook-jako-spion-prozradi-o-vas-uplne-vsechno

Facebook toho o vás ví mnohem víc, než si myslíte. *Eurozpravy.cz* [online]. 2009, 03. dubna 2015 [cit. 2016-01-18]. ISSN 2336-257X. Dostupné z: http://veda-a-technika.eurozpravy.cz/internet/117195-facebook-toho-o-vas-vi-mnohem-vic-nez-si-myslite

Forenzní věda (Forenzika). *Management Mania* [online]. 2011, 10.05.2013 [cit. 2016-01-21]. Dostupné z: https://managementmania.com/cs/forenzni-veda-forenzika-forensics

Get your Data!. *Europe versus Facebook* [online]. Austria, 2012 [cit. 2016-01-24]. Dostupné z: http://europe-v-facebook.org/EN/Get_your_Data_/get_your_data_.html

Ghostery. *Jak na webové stránky - Zvyšování výkonu a bezpečnost webových stránek* [online]. 2005, 19.11.2015 [cit. 2016-02-28]. Dostupné z: http://timehosting.cz/ghostery/

HEIN, Jakub. Internet už dávno není anonymní. In: *CCIZ* [online]. 2013, 6.2.2015 [cit. 2016-01-17]. Dostupné z: https://www.investigace.cz/internet-uz-davno-neni-anonymni

HENRY, Alan. The Best Browser Extensions that Protect Your Privacy. *Lifehacker* [online]. 2005, 2015-08-31 [cit. 2016-02-28]. Dostupné z: http://lifehacker.com/the-best-browser-extensions-that-protect-your-privacy-479408034

HNÁT, Ondřej. Uživatel, cookie, sledování a remarketing – kde jsou hranice? *Sunitka* [online]. 2010, 24. prosince 2013 [cit. 2016-01-19]. Dostupné z: http://www.sunitka.cz/c/632-uzivatel-cookie-sledovani-a-remarketing-kde-jsou-hranice

How To Protect Your Data And Remove Personal Information From The Internet. *Abine* [online]. 280 Summer St. Boston, 2015 [cit. 2016-02-26]. Dostupné z: https://www.abine.com/optouts.php

CHAPMAN, Cameron. How to permanently delete your account on popular websites. *Smashing Magazine* [online]. 2016, June 11th, 2010 [cit. 2016-02-26]. Dostupné z: https://www.smashingmagazine.com/2010/06/how-to-permanently-delete-your-account-on-popular-websites/

CHRISTENSSON, Per. Digital Footprint. *Techterms* [online]. 2005, May 26, 2014 [cit. 2016-01-20]. Dostupné z: http://techterms.com/definition/digital_footprint

ICT Facts and Figures – The world in 2015. *ITU* [online]. 2015 [cit. 2015-11-19]. Dostupné z: http://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx

JonDo Help: JonDonym. *JonDonym - the anonymisation service* [online]. 2006 [cit. 2016-02-28]. Dostupné z: https://anonymous-proxy-servers.net/en/help/jondonym.html

JANOVSKÝ, Dušan. Logy ze serveru. *Jakpsátweb* [online]. 1998 [cit. 2016-01-20]. ISSN 1801-0458. Dostupné z: http://www.jakpsatweb.cz/seo/logy.html

KRATOCHVÍL, Petr. Anonymní surfováni. *Chip* [online]. Německo: CHIP Communications, 2016, 02.07.2013 [cit. 2016-02-28]. ISSN 0170-6632. Dostupné z: http://www.chip.cz/casopis-chip/earchiv/rubriky/technika/anonymni-surfovani/

Krádež identity a jak se jí bránit. *Bezpečný internet.cz* [online]. [cit. 2016-01-21]. Dostupné z: http://www.bezpecnyinternet.cz/pokrocily/ochrana-prav/kradez-identity.aspx

KRUSE, Warren G a Jay G HEISER. *Computer forensics: incident response essentials*. Boston, MA: Addison-Wesley, 2001, xiii, 392. ISBN 0201707195

Log (log file). *Whatis.com* [online]. 1999 [cit. 2016-01-20]. Dostupné z: http://whatis.techtarget.com/definition/log-log-file

MARTÍNEZ-CABRERA, Alejandro. Erasing all digital footprints 'impossible'. *San Francisco chronicle* [online]. San Francisco, Calif.: Chas. D. Young, July 6, 2010 [cit. 2012-05-14]. ISSN 1932-8672. Dostupné z: http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2010/07/05/BU4V1E8D9V.DTL

NOVÁK, Michal. Jaké informace o vás Google shromažďuje. In: *SPRÁVA-SÍTĚ.com* [online]. 2016, 7.9.2015 [cit. 2016-01-17]. Dostupné z: http://www.sprava-site.com/jake-informace-o-vas-google-shromazduje-2353

O'REILLY, Tim. What Is Web 2.0. *O'reilly* [online]. 2005 [cit. 2015-11-19]. Dostupné z: http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html

Prozkoumejte své záznamy o aktivitách. *Facebook* [online]. 2010 [cit. 2016-01-23]. Dostupné z: https://www.facebook.com/help/437430672945092

ROUSE, Margaret. Metadata. In: *Whotis.com* [online]. 1999, červenec 2013 [cit. 2016-01-17]. Dostupné z: http://whatis.techtarget.com/definition/metadata

STOCKLEY, Mark. How to clear out cookies, Flash cookies and local storage. *Naked Security* [online]. 1985, 05 NOV 2014 [cit. 2016-02-27]. Dostupné z: https://nakedsecurity.sophos.com/2014/11/05/how-to-clear-out-cookies-flash-cookies-and-local-storage

STRNAD, Zdeněk. Zmizet není snadné, ale jde to. *E15* [online]. 2007, 23.3.2015 [cit. 2016-01-20]. ISSN 1210-1168. Dostupné z: http://zen.e15.cz/telegraf/zmizet-neni-snadne-ale-jde-to-1169387

The Ultimate Guide to the Invisible Web. In: *Open Education Database (OEDb)* [online]. 2006, 11. 11. 2013 [cit. 2016-01-22]. Dostupné z: http://oedb.org/ilibrarian/invisible-web

TKAČÍKOVÁ, Daniela. Neviditelný web. In: *KTD: Česká terminologická databáze knihovnictví a informační vědy (TDKIV)* [online]. Praha: Národní knihovna ČR, 2014 [cit. 2016-01-22]. Dostupné z: http://aleph.nkp.cz/F/?func=direct&doc_number=000000547&local_base=KTD

TONY FISH. *My digital footprint: a two sided digital business model where your privacy will be someone else's business* [online]. London: Futuretext, 2009 [cit. 2016-01-17]. ISBN 09-556-0698-5

Tor Metrics - Relays with Exit, Fast, Guard, Stable, and HSDir flags. *Tor Metrics* [online]. 2004, 2016-02-28 [cit. 2016-02-28]. Dostupné z: https://metrics.torproject.org/relayflags.html

Tor Project: Overview. *Tor Project: Anonymity Online* [online]. 2004 [cit. 2016-02-28]. Dostupné z: https://www.torproject.org/about/overview.html.en

Total number of Websites & Size of the Internet as of 2013 : Facts Hunt. *Facts Hunt* [online]. 2016 [cit. 2016-03-07]. Dostupné z: http://www.factshunt.com/2014/01/total-number-of-websites-size-of.html

Tutorials. *AdBlock Plus* [online]. [cit. 2016-02-28]. Dostupné z: https://adblockplus.org/en/tutorials

V síti datových dealerů. *Chip* [online]. 1978, **2013**(04) [cit. 2016-03-07]. ISSN 0170-6632. Dostupné z: http://www.chip.cz/casopis-chip/earchiv/vydani/rocnik-2013/chip-04-2013/v-siti-dat/

VŠETEČKA, Roman. Do konce roku bude k internetu připojena téměř polovina obyvatel Země.*Technet.cz* [online]. 1999, 27. května 2015 [cit. 2015-11-19]. Dostupné z: http://technet.idnes.cz/celosvetove-pripojeni-k-internetu-dtx-/sw_internet.aspx?c=A150527_114416_sw_internet_vse

W3Counter: Global Web Stats - January 2016. *W3Counter* [online]. 2004 - 2016, January 2016 [cit. 2016-02-27]. Dostupné z: http://www.w3counter.com/globalstats.php?year=2016&month=1

WALLACE, Mark. Recruiting on Facebook: How to Ethically Screen Candidates. *Akken Cloud* [online]. 12. 08. 2015 [cit. 2016-01-21]. Dostupné z: http://www.akkencloud.com/recruiting-on-facebook/

WILLIAMS, Ben. Adblock Plus and (a little) more. *AdBlock Plus* [online]. 2015-05-27 [cit. 2016-02-28]. Dostupné z: https://adblockplus.org/blog/another-court-another-obvious-win-for-ad-blocking-and-acceptable-ads-too

YALE, Brad. How the Internet Works: The Deep Web. *InformIt* [online]. 21 října 2014 [cit. 2016-03-07]. Dostupné z: http://www.informit.com/blogs/blog.aspx?uk=How-the-Internet-Works-The-Deep-Web

Zobrazení dat a aktivity na účtu na Hlavním panelu Google. *Google* [online]. 1998 [cit. 2016-01-24]. Dostupné z: https://support.google.com/accounts/answer/162744?hl=cs

Ztráta identity. *Policie České republiky* [online]. 2015 [cit. 2016-01-21]. Dostupné z: http://www.policie.cz/clanek/ztrata-identity.aspx