Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Naše digitální stopa na počítači a na Internetu

Autor: Michal Kleinander

Vedoucí práce: Ing. Čestmír Halbich, CSc.

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Michal Kleinander

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 02. 03. 2016

Čestné prohlášení

Prohlašuji, že jsem svou bakalářskou práci „Naše digitální stopa na počítači a na Internetu“ 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 ….….. Podpis ..….....

Poděkování

Rád bych touto cestou poděkoval vedoucímu bakalářské práce panu Ing. Čestmíru Halbichovi, CSc., za cenné rady a připomínky a jeho vstřícný přístup během zpracovávání mé bakalářské práce. V neposlední řadě patří díky i celé mé rodině a známým za podporu při vypracovávání práce.

Naše digitální stopa na počítači a na Internetu

Digital footprint on own computer and the Internet

Souhrn

Tato bakalářská práce se zaměřuje na digitální stopy a jejich ochranu. V kapitolách jsou stručně popsány základní pojmy včetně rozdělení digitálních stop. Dále jsou popsána případná rizika a hrozby, ke kterým může dojít při zneužití digitálních stop. Teoretická část je uzavřena způsoby, kterými lze kontrolovat digitální stopy a dále správou digitálních stop včetně přehledu nástrojů. Praktická část je již zaměřena na testování a komparaci vybraných nástrojů pro ochranu soukromí. Na základě porovnání nástrojů je stanoveno vhodné řešení ochrany digitální stopy.

Summary

This work is focused on digital footprint and security. The basic terms and distribution of digital footprints are briefly described in the chapters. There are also described potential risks and threats that may occur due to misuse of digital footprints. The theoretical part is ended by the ways to control digital footprints and their management including the overview of tools. The practical part is focused on testing and comparison of selected tools for privacy protection. On the basis of comparison tools is provided a suitable solution in protection of digital footprint.

Klíčová slova: Digitální stopa, ochrana dat, soukromí, hesla, cookies

Keywords: Digital footprint, protection of personal data, privacy, passwords, cookies

Obsah

1 Úvod

V dnešní době používá internet obrovská masa lidí. Internet se stal naším běžným každodenním pomocníkem, bez kterého by se spousta lidí neobešla. S rozšířením chytrých telefonů, tabletů a dalších zařízení došlo k jeho ještě většímu využití. Každý chce být neustále připojen a být tzv. „online“.

Internet nám nabízí nepřeberné možnosti. Pomocí něho můžeme jednoduše komunikovat s ostatními, hledat nová přátelství na sociálních sítích, hledat nové informace, nakupovat elektronicky, sebevzdělávat se a mnoho dalších věcí.

V dnešní době již neplatí, že internet ovládají pouze dospělí, technicky zdatní lidé. Internet se stal globálním fenoménem 21. století. Internet stále více využívá mladší generace, především děti a mladiství. S tím souvisí i určitá pravidla chování na internetu, která by měla být dodržována.

Na internetu má většina lidí pocit anonymity a beztrestnosti. Tak to ovšem úplně není. Každý z nás by si měl uvědomit, že co na internet umístí, lze jen velmi těžko smazat. Dále by si měl každý uvědomit a dobře promyslet, jaké informace chce o sobě na internetu sdílet. To znamená, každý by měl dbát na to, aby po sobě zanechával „zdravou“ digitální stopu.

Toto téma bakalářské práce bylo vybráno především kvůli jeho aktuálnosti. Prevence ochrany našich dat a soukromí na internetu je a bude téma i do budoucna.

2 Cíl práce a metodika

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, funkcí, požadavků a možností navrhnout a implementovat vhodné řešení individuální ochrany dat.

Teoretická část se zabývá především vznikem a rozdělením digitálních stop a dále případnými riziky a hrozbami při zneužití digitálních stop. Dále jsou popsány možnosti kontroly digitálních stop a jejich eliminace. Praktická část je zaměřena na porovnání vybraných volně dostupných nástrojů dle kritérií a oblastí, kterými se zabývají.

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

3 Vymezení základních pojmů

V prvé řadě je třeba si nejdříve definovat klíčové údaje, se kterými budu dále pracovat. Prvním tímto termínem, který nejvíce souvisí s mojí prací, je pojem Digitální stopa, její definice a dělení. S tímto pojmem úzce souvisí i pojem Osobní údaj jako primární informace o identifikaci každého z nás a pojem Soukromí na internetu jako klíčový prvek ochrany dat v souvislosti s naší digitální stopou.

3.1 Digitální stopa

„Digitální stopa je jakákoliv informace s vypovídající hodnotou, uložená nebo přenášená v digitální podobě.“ [1]

Tato definice zahrnuje všechny oblasti digitálních technologií. Pokrývá tedy jak oblast počítačů, tak i oblast digitálních přenosů (mobilní telefony), videa, audia, data kamerových

[1] RAK, Roman a Viktor PORADA. Teorie d*igitálních stop a její aplikace v kriminalistice a forenzních vědách*. Karlovarská právní revue č.4. 2006. s. 5. ISSN 1801-2193

systémů atp. Každé technologické zařízení, které získává, zpracovává nebo uchovává data po sobě, zanechává určité záznamy (stopy). [2]

Někdy se také setkáváme s pojmem počítačová stopa, který je již zastaralý, protože stopy zanecháváme i na jiných zařízeních, než jsou počítače. Tento pojem vznikl současně s pojmem počítačová kriminalita, přibližně ve druhé polovině 80. let 20. století.

V zahraniční literatuře je digitální stopa definována jako „digital evidence“ či „digital footprint“.

3.1.1 Rozdělení

Digitální stopy jsou spojovány s mnoha obory. Jako příklad bych uvedl dva obory - kriminalistika a forenzní vědy a informační technologie. Mohli bychom porovnávat více oborů, ale myslím, že pro názornost rozdělení tyto dva postačí.

3.1.1.1 Kriminalistika a forenzní vědy

V kriminalistice a forenzních vědách jsou digitální stopy brány především jako důkazní materiály. Využití zde nacházejí nejen při dokazování trestných činů, ale i při forenzních šetřeních či občanskoprávních sporech. Zde však dochází ke sporům, kdy jedna strana považuje za digitální stopu data, která jsou spojena přímo s trestným činem. Druhá skupina považuje za digitální stopu informace, která mají vypovídací hodnotu a jsou přenášená v digitální podobě. Do této skupiny bychom zahrnuli především „otisky“, které za sebou zanechávají technologická zařízení pracující s daty. Kupříkladu seznam hovorů v telefonu, kamerové videozáznamy nebo třeba i datum a čas pořízení fotografie.

3.1.1.2 Informační technologie

Již slovo „digitální“ stopa, vykazuje samo o sobě vztah k informačním technologiím, počítačům a dalším elektronickým zařízením. Společným znakem těchto zařízením je především jejich možnost přístupu k internetu. Tímto pohybem a činnostmi uživatele v prostředí internetu vznikají právě digitální stopy. Digitální stopu tedy tvoří určitý soubor informací, které po sobě zanechává uživatel používající internetovou síť. Tyto informace po sobě zanecháváme buď vědomě, nebo nevědomě. Proto můžeme dělit digitální stopy v této oblasti na dvě skupiny: aktivní a pasivní.

[2] FISH, Tony. My digital footprint: a two sided digital business model where your privacy will be someone else's business. ISBN 978-095-5606-984.

Aktivní digitální stopy jsou informace vědomě zanechané samotným uživatelem. Jedná se především o příspěvky a komentáře na veřejných stránkách, osobní webové stránky, fotografie a videa nahraná a sdílená prostřednictvím serverů či členství v zájmových skupinách a fórech, profily na sociálních sítích, emaily, sms, historie chatu apod.

Pasivní digitální stopy jsou informace, které o sobě uživatel nevědomě zanechává při jeho „pobytu“ na internetu. Zde se jedná především o záznamech aktivit uživatele v online prostředí, datech představující výčet navštívených webových stránek, četnosti a časech jejich návštěv dále pak uživatelovi činnosti na jednotlivých stránkách, uložení jeho IP adresy a lokace.

3.2 Osobní údaj

„Jakákoliv 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.“ [3]

Osobní údaj je tedy informace, která se týká fyzické osoby, k níž se vztahují osobní údaje.

Rysem osobního údaje je, že jednoznačně vypovídá informace o dané určité osobě a zároveň tyto informace nelze přiřadit žádné jiné osobě. Platí tedy, že pokud může být osoba z nashromážděných údajů identifikována, pak se jedná o osobní údaj.

Identifikace přímá se týká údajů, které jasně prokazují identitu a mají jasnou vypovídací hodnotu. Například jméno osoby, příjmení, datum narození, rodné číslo.

Identifikace nepřímá je založena na identifikování osoby bez uvedení jejího jména. Může se jednat tedy o identifikaci na základě neobvyklého povolání osoby, jeho zdravotního stavu apod.

3.3 Soukromí na internetu

Soukromí reálného života a soukromí na internetu se od sebe zásadně liší. Je to především díky tomu, že soukromí uživatelů na internetu bývá velmi často podceňováno a

3 § 4 písm. a) Zákona č. 101/2000 Sb., o ochraně osobních údajů

zanedbáváno. Lidé si na internetu ve virtuálním světě tvoří své „druhé já“ kterému se snaží přikládat svou vlastní reálnou osobnost. Spousta lidí tak žije vlastně dva životy, jeden reálný a druhý virtuální.

Virtuální svět od uživatelů v mnoha případech vyžaduje sdělení jejich reálných informací, kým jsou, kde pracují, jaké mají záliby atp.

Je zajímavé, že lidé v reálném světě si tyto informace celkem dost chrání, jsou nedůvěřiví vůči cizím lidem a ostýchaví. Existuje taková přirozená nedůvěra, která nás svým způsobem ochraňuje před zneužitím našich osobních informací a osobnosti.

Tato nedůvěra však ve virtuálním světě z obrovské části mizí. Především na sociálních sítích, kde o sobě lidé sdílejí spoustu informací, aniž by si uvědomili (ve většině případů), že se mohou vystavovat celkem velkému riziku vyzrazení jejich údajů. Stačí v zásadě jedno kliknutí a pohled a o dané osobě si uděláme sami svůj vlastní obrázek.

Dle mého názoru bychom měli striktně oddělovat naše reálné soukromí od soukromí internetového. Měli bychom na internetu dávat daleko větší pozor na naše soukromí, oproti reálnému životu, protože informace o nás sdělené na internetu jsou daleko snáze zjistitelné a průkazné.

4 Lokální data na počítači

V této části bude řeč především o metodách, které ukládají informace o nás (naší digitální stopě) na náš disk (hardware).

4.1 Cookies

První cookies byly vytvořeny v roce 1994. Vytvořil je americký programátor Lou Montulli. Do tohoto roku byl web bez jakékoli „paměti“, takže opuštění stránky vedlo k nemožnosti navázání na ní při další návštěvě. Web tedy nemohl uživatele žádným způsobem identifikovat a přerušení znamenalo vykonání celé operace znovu. Problém byl vyřešen tak, že byla webovým stránkám dána možnost uložit textový soubor do uživatelova počítače. Soubor obsahuje unikátní ID a informace, které umožňují vzájemnou identifikaci mezi webem a počítačem.

Cookies patří do pasivní digitální stopy, kdy o sobě ukládáme (většina uživatelů nevědomě) naší aktivitu při pohybu na internetu. Jedná se o malé soubory, které se při naší první návštěvě webové stránky ukládají na hard disk počítače. V praxi nám dovolují ukládat například naše přihlašovací údaje, personalizovat oblíbené stránky nebo používat nákupní košík v elektronických obchodech. Obsahují informace, jak často uživatel navštěvuje danou stránku, jakými hesly a jmény se přihlašuje.

Původní účel cookies měl usnadnit uživatelům práci s webovými stránkami a zlepšit jejich celkovou funkčnost. Bohužel lze tyto údaje využít i k jiným účelům. Pomocí nich lze monitorovat pohyb uživatele a tím i zjišťovat jeho zájmy a pomocí nich pak na něj cílit reklamu. Některé webové stránky využívají cookies, které umožňují sociálním sítím vidět polohu uživatele, zařízení, ze kterého je připojen, ale i počet kliknutí a dobu připojení. Na základě takto zjištěných informací jsou pak uživateli nabízeny reklamy a odkazy, které by ho mohli zajímat.

4.1.1 Druhy Cookies

Rozlišujeme dva druhy cookies dle jejich vlastníka a původu:

4.1.1.1 1st party cookies

Vlastníkem tohoto typu je vždy webová stránka, ta je ukládá do počítače (pomocí skriptu na dané doméně) pro příští návštěvu uživatele. Lze také uložit preferované nastavení na dané webové stránce. Tyto cookies jsou bezpečnější než druhý zmíněný typ. Tento typ používá například systém Google Analytics.

4.1.1.2 3rd party cookies

Vlastníkem tohoto druhého typu jsou třetí strany. Cookie je uložena za pomoci skriptu, který je natáhnut do webu z jiné domény. Tyto uložené cookies mohou identifikovat uživatelův počítač na všech webech, které spravuje agentura (cross site tracking). Uživatelův pohyb je tak bez jeho vědomí sledován. Tyto cookies zpravidla ukládají informace o tom, co konkrétně uživatel na jejich webu prohlížel nebo také informace o poslední návštěvě stránky. Takto společnosti získávají údaje o zájmech uživatelů. Cookies obvykle neobsahují citlivé osobní informace o uživateli za předpokladu, pokud je sám webové stránce neposkytl. V tomto případě může dojít k zásahu do soukromí uživatele. Tento typ používá systém NetMonitor.

4.1.2 Flash Cookies

Jiným názvem také „lokální sdílené objekty“ (LSO). Jedná se o druh cookies, které do počítače ukládají aplikace využívající Adobe Flash. Flash umožňuje využití grafických animací, bannerů, hraní her, přehrávání videí na webových stránkách (je třeba nainstalovat modul Adobe Flash Player). Flash cookies mají plnit funkce stejné jako klasické http cookies. I přesto je ale většina webů používá ke sledování aktivit uživatelů.

Flash cookies mají oproti http cookies několik negativních vlastností. Klasické mazání cookies prostřednictvím internetového prohlížeče nemá na flash cookies žádný vliv, protože jsou uložené na počítači v samostatné složce:

```
C:\Users\<uživ.jméno>\AppData\Roaming\Macromedia\Flash Player\#SharedObjects
```

Vzhledem k jejich neomezené expirační době tak mohou zůstat uložené v uživatelově počítači velmi dlouho. Ukládají mnohonásobně více dat oproti klasickým cookies (až 100 KB). Také nejsou vázány na konkrétní prohlížeč a tím dovolují třetím stranám sledovat pohyb uživatele nejen mezi weby, ale i prohlížeči. [4]

Podobným typem k flash cookies jsou i Silverlight cookies, které fungují na totožném principu a lze je nalézt ve složce:

```
C:\Users\<uživ.jméno>\AppData\LocalLow\Microsoft\Silverlight
```

4.2 Historie procházení

Každý internetový prohlížeč si ukládá samostatně uživatelovu historii procházení jednotlivých webů chronologicky podle času. V historii se však neukládají zabezpečené stránky webů (internetbanking atd.). Dále se do historie procházení neukládají stránky navštívené pomocí anonymního režimu prohlížeče.

Dále platí, že pokud používáme jeden a ten samý prohlížeč na více zařízeních a jsme na něm přihlášeni, bude se nám historie zobrazovat a synchronizovat ze všech zařízení. Například u Chromu uživatel ráno surfuje po internetu na PC a poté ho vypne. Odpoledne

[4] ČÍŽEK, Jakub. *Flash prý skrývá nebezpečí, říká se mu Flash Cookies* [online].

si uživatel zapne notebook, otevře si Chrome a v historii uvidí, na jakých stránkách ráno byl a může si je zpětně načíst.

V historii se neukládá pouze procházení jednotlivých webových stránek. Ukládá se tam dále například historie formulářů, kam patří údaje, které jsme zadávali do formulářů na webových stránkách a které nám může prohlížeč nabízet k předvyplnění u budoucích formulářů (tzv. automatické vyplňování formulářů). Dále se do historie ukládají aktivní přihlášení na webových stránkách (po přihlášení uživatele k zabezpečené webové stránce je přihlášení označeno jako aktivní). Také některá cookies se mohou ukládat do historie (záleží na prohlížeči). Dále lze v historii uložit i offline obsah webové stránky, pokud si ho povolíme v nastavení prohlížeče.

Např. Google Chrome ukládá historii do:
`C:\Users\<uživ.jméno>\AppData\Local\Google\Chrome\User Data\Default\History`

Historii by měl uživatel pravidelně promazávat, předejde se tak pomalejšímu načítání webových stránek a zneužití soukromí.

4.3 Uložená hesla

Spousta dnešních prohlížečů nabízí uživatelům možnost uložit si a zapamatovat jejich hesla k účtům. Spousta lidí této funkce na jejich desktopu nebo noteboocích využívá. I tak to nese ale mnoho bezpečnostních rizik.

V zásadě si každý prohlížeč uchovává hesla do jednoho souboru. Hesla si pak lze v jednotlivých prohlížečích prohlížet v nastavení prohlížeče, jak píše pan Dočekal. [5] Uložená hesla se tak zobrazí v přehledné tabulce, ovšem s hvězdičkami. Pak již stačí dát vpravo Zobrazit. Zobrazení hesel ale ještě vyžaduje autentizaci účtu, pod kterým jste přihlášeni k PC (viz Obrázek 1). Toto ověření částečně zvyšuje ochranu, protože případný útočník by musel nejprve znát vaše heslo k počítačovému účtu a až poté by zjistil hesla k vašim zapamatovaným heslům.

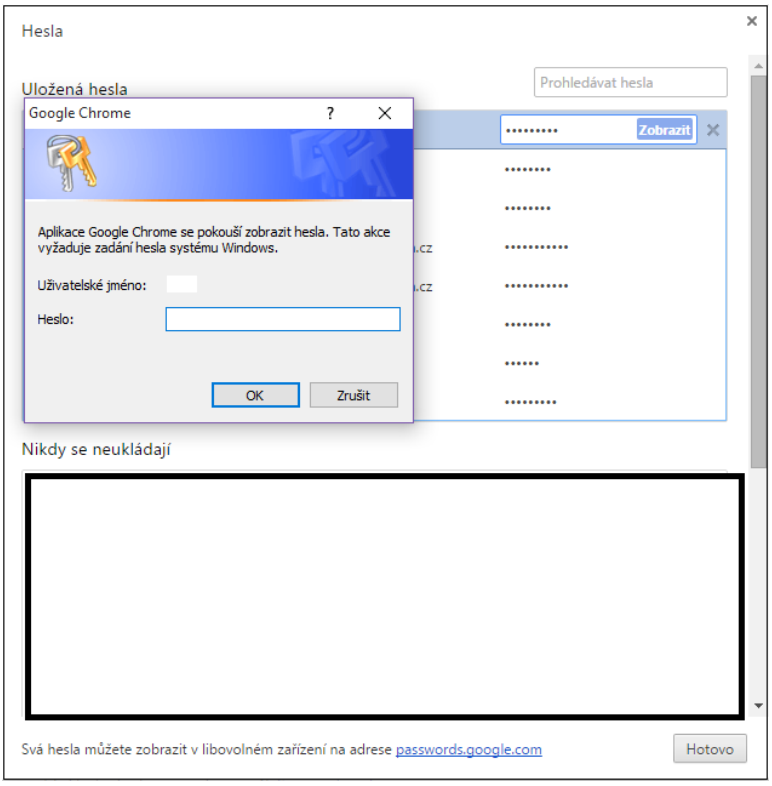
[5] DOČEKAL, Daniel. *Hesla uložená v prohlížeči Chrome lze získat „až překvapivě snadno“* [online].

Dále lze k zobrazení hesel použít software třetích stran. Příkladem může být program od společnosti Nirsoft WebBrowserPassView. Ten je freeware a umožňuje přehledně zobrazit všechna uložená hesla ze všech prohlížečů. [6]

V žádném případě by uživatelé neměli ukládat svá hesla v prohlížečích na cizích počítačích, kde je vytvořen jeden účet pro všechny příchozí uživatele (např. knihovny, školy atp.). Velmi se tím zvyšuje riziko zneužití a odhalení hesla a s tím i získání citlivých údajů o uživateli.

Uložená hesla v Google Chromu se ukládají do:

`C:\Users\<uživ.jméno>\AppData\Local\Google\Chrome\User Data\Default\Login Data`



Obrázek 1 - Požadavek zadání uživatelského hesla v Google Chrome (zdroj: vlastní archiv autora)

[6] ČÍŽEK, Jakub. *Jak odhalit uložená hesla v Chromu během několika sekund* [online].

5 Internet

V následující části se bakalářská práce zabývá především způsoby, které zanechávají informace o nás (naší digitální stopě) na internetu. Ať už na sociálních sítích nebo obecně v rámci sítě internet.

5.1 Sociální síť

Pojem sociální síť lze definovat mnoha způsoby, avšak základem každé té definice je to, že sociální síť je virtuální prostor, kde uživatelé mohou „žít“ svůj život ve virtuálním světě.

Sociální sítě nám umožňují nespočet věcí, ať již komunikaci s našimi přáteli, sdílení našich fotek, videí, pocitů, stavů a informací o nás s ostatními. Můžeme říci, že lidé přenášejí své reálné sociální sítě a hodnoty do virtuálního kyberprostoru. Jak již bylo řečeno v úvodu práce, lidé se cítí v prostředí internetu a tedy i na sociálních sítích anonymní. Uživatelé si mohou vylepšovat jejich vlastnosti oproti pravdivé realitě, aniž by to kdokoli poznal (krom přátel, kteří je znají osobně).

Sociální sítě nabízejí mnoho výhod. Hlavní výhodou je rychlá a bezplatná komunikace s kýmkoli po celém světě. S touto komunikací souvisí i interakce mezi jednotlivými uživateli, kdy si mohou posílat zajímavé fotky, odkazy, pozvánky na akce atd.

Sociální sítě mají však i své nevýhody. Uživatelé se mohou stát například závislí na sociálních sítích. Dále pak může dojít k narušení soukromí uživatelů (Viz kapitola 5; Stalking, krádež identity, kyberšikana)

5.1.1 Dělení sociálních sítí

Sociální sítě jsou rozděleny na dvě skupiny. První skupinu tvoří sociální sítě, které se zaměřují na tvorbu uživatelova profilu. Druhou pak sítě, kde uživatelé tvoří vlastní obsah a sdílejí ho s ostatními uživateli internetu.

5.1.1.1 Profilové sociální sítě

Jak již bylo řečeno, tyto sociální sítě se zaměřují především na tvoření uživatelských profilů, jejich vzájemné interakci. Uživatelé zde spolu sdílejí své koníčky, diskutují o svých zájmech. Sdílejí zde své fotky, videa, pocity, názory, nálady s ostatními, žijí zde

tedy svůj druhý „virtuální“ život. Tyto sítě patří k jedněm z nejoblíbenějším sociálním sítím na internetu.

Jako příklad lze uvést např. všem dobře známý Facebook, jako celosvětově nejvíce používanou sociální síť nebo Google+. Z českých profilových sociálních sítích bych uvedl Lide.cz nebo Hotnot.cz

Sítě se neustále vylepšují, ať už po grafické stránce nebo po funkční. Vývojáři se snaží tyto sítě implementovat i do jiných zařízení jako jsou chytré telefony, tablety, televize a další. Tím vlastně předčili původní staré programy pro komunikaci jako ICQ, Jabber, které už se vesměs nepoužívají, protože každý uživatel raději komunikuje přes Messenger, který spojuje informace z facebookového účtu uživatele se seznamem jeho přátel.

5.1.1.2 Obsahové sociální sítě

Tyto sociální sítě se v takové míře nezaměřují na profily uživatelů, ale zaměřují se na obsah vytvářený samotnými uživateli. Bývají tedy zaměřené na jedno konkrétní téma (hudba, profesní život apod.) čímž se liší od profilových, které toto vše zastávají v jednom rozhraní. Dříve bývaly tyto sítě nezávislé na profilových sociálních sítích, ale s rostoucí popularitou Facebooku došlo k jejich propojení.

Příkladem obsahových sociálních sítí je kupříkladu Youtube, který slouží uživatelům hlavně k vytváření a šíření jejich obsahu a sledování obsahu jiných. Youtube se tedy především orientuje na sdílení hudebních videí a videí obecně. Další obsahovou sociální sítí je Instagram. Ten se zaměřuje především na vytváření a sdílení fotek uživatelů s celým světem. Obrázky zde nahrané se značí # (hashtagem), na jehož principu funguje hledání podobných fotek jako je název námi hledaného hashtagu. Co se týče dalších obsahových sociálních sítí, lze jmenovat například Twitter, sloužící především pro psaní mikroblogů. Dále profesní síť LinkedIn, která se zaměřuje na hledání nových pracovních míst a profesních kontaktů. Jako poslední bych uvedl českou síť Spolužáci, která se zaměřuje především na zkontaktování bývalých lidí ze školy nebo z vojny.

5.1.2 Pluginy sociálních sítí

Pluginy sociálních sítí (social plugins) slouží k získání přehledu o aktivitách na internetu. Jedná se o aplikace, které obsahují webové stránky a umožňují provázání sociálních sítí s webovými stránkami. V praxi to pak vypadá tak, že pokud je uživatel přihlášen na jeho

sociální síti, může na stránce s pluginem například komentovat příspěvky pod jeho profilem ze sociálních sítí. Dále může sdílet příspěvky na sociálních sítích, používat tlačítka „To se mi líbí“ (Facebook), +1 (Google+) a dalších. [7]

Z článku od Toma Simonita[8] vyplývá, že pluginy na webových stránkách jako „To se mi líbí“ či „Sdílet“ začnou poskytovat data o zájmech uživatelů jednotlivým společnostem. Tyto společnosti budou poté na základě takto poskytnutých dat o jednotlivých uživatelích a jejich zájmech předhazovat relevantní reklamu „na míru“ každému uživateli. Rainey Reitman tvrdí, že již při návštěvě uživatele na webu s „To se mi líbí“ pluginem jsou odesílány informace o zájmech uživatele. Tyto informace se odvíjí od tématu stránky. Tímto dochází opět k sledování aktivit uživatele na internetu a k částečnému zásahu uživatele do jeho soukromí.

5.2 Hrozby při pohybu v síti Internet

Při našem pohybu na internetu nás ohrožuje mnoho hrozeb a spousta uživatelů si to ani neuvědomuje. Je to především v důsledku malé informovanosti uživatelů o těchto hrozbách. Spousta lidí, chodící na internet, tato rizika zpravidla vůbec nevnímá nebo o nich dokonce ani neví. Toto bohužel velmi ulehčuje „práci“ internetovým podvodníkům, pro které jsou tito málo informovaní uživatelé snadnou kořistí.

Důležitou pozornost by měli uživatelé věnovat nastavení jejich soukromí v rámci sociální sítě. Většina uživatelů si založí svůj profil na sociálních sítích a nevěnují pozornost nastavení jejich soukromí. Zvláště u sociální sítě Facebook, kde lze téměř u všech informací o nás nastavit, kdo přesně tyto informace uvidí a kdo naopak ne.

Proto je třeba popsat rizika, se kterými se mohou uživatelé setkat na internetu a na sociálních sítích. Dále popíši, jak se proti těmto útokům bránit, případně se jim úplně vyhnout.

5.2.1 Spam

„Jako spam se na internetu označuje veškerá nevyžádaná pošta, tj. hromadně zasílané emaily, jejichž úkolem je především šířit reklamní sdělení.“ [9]

[7] HINES, Kristi. *Facebook for Websites: Social Plugins for Your Blog and Business* [online].
[8] SIMONITE, Tom. *Facebook's Like Buttons Will Soon Track Your Web Browsing to Target Ads* [online].
[9] Citace z: http://www.adaptic.cz/znalosti/slovnicek/spam/

Hlavním znakem spamu je, že je téměř nemožné ho zrušit. Uživatelovi tak chodí neustálý přísun těchto zpráv, protože je jeho e-mailová adresa zařazena v databázi společnosti, co spamy rozesílá. Obsahy spamu jsou různorodé, většinou se jedná o nabídku zboží či služeb. Tyto spamové zprávy tak chodí uživateli na jeho mail velmi často. Naštěstí však existují tzv. spamové filtry [10], které dokáží filtrovat spamové zprávy na základě zadání klíčových slov a slovních spojení. I přesto rozeznání spamu pomocí filtru není 100 % a filtr může označit jako spam zprávy, které spamem vůbec nejsou.[11]

Proti spamu lze bojovat legislativní cestou. Existuje totiž Antispamový zákon přesněji Zákon č. 480/2004 Sb., *o některých službách informační společnosti a o změně některých zákonů*, který nám umožňuje nahlásit podezřelé e-maily na Úřad pro ochranu osobních údajů (ÚOOÚ). Ten by měl zprávy prověřit a případně zakročit proti rozesílateli.

S rozšířením sociálních sítí se spameři začali zaměřovat nejen na podvodné a obtěžující zprávy do e-mailových schránek uživatelů, ale i na zprávy na sociálních sítí. Spameři zde zveřejňují spamové komentáře s odkazy na externí webové stránky s výrobky. Dále si zde mohou vytvořit smyšlený profil a přidávat si náhodné přátele na profil a odesílat jim odkazy na externí stránky, kdy může dojít i k phishingovému útoku (viz Phishing). Příkladem může být situace, kdy příchozí e-mail zval uživatele na sociální síť Google+. E-mail vypadal téměř stejně jako od Googlu, avšak po kliknutí na odkaz na sociální síť nevedl na sociální síť, nýbrž na stránku s farmaceutickými výrobky [12]

Nejlepším řešením proti spamu je mít více e-mailových adres a oddělit tak osobní e-mailovou schránku a schránku na „spamy“. Veškeré registrace tedy provádět na druhý „spamový“ e-mail, kam budou chodit akce, newslettery a další obchodní nabídky, zatímco osobní e-mail zůstane těmito spamy nedotčen.

5.2.2 Phishing

Phishing vyplývá z anglického slova fishing, tedy rybaření (rhybaření). Tento způsob útoku funguje v zásadě na tom samém principu. Útočník (rybář) nahodí udičku a čeká, který uživatel (ryba) se na ní chytí.

[10] FIŠEROVÁ, Kateřina. *Spamový filtr* [online].
[11] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. s. 124. ISBN 80-251-0106-1.
[12] MCMILLAN, Robert. *Spam messages promise Google+ invites, deliver drug ads* [online].

Tento útok spočívá v obdržení podvodného e-mailu, který má za cíl vzbudit dojem, že byl odeslán z oficiálního e-mailu společnosti. Zpráva vyzývá k zaslání osobních údajů (hesel, bankovních účtů atd.). Phishingová zpráva může vypadat jako výzva k aktualizaci bezpečnostních údajů, informace o neprovedené platbě apod. Jejím cílem je tedy získat od oběti přihlašovací údaje a údaje o platebních kartách.

Jedním typem obrany proti phishingu je ověření e-mailové adresy, ze které přišel daný e-mail. Další obranou je na tyto maily neodpovídat a už vůbec posílat naše citlivé údaje. [13]

5.2.3 Pharming

Podobnou technikou k phishingu je pharming (farmaření). Principem je napadení DNS [14] a přepsání IP adresy. Pokud tedy uživatel zadá webovou adresu, nedojde k překladu na odpovídající IP adresu, nýbrž na jinou (podvodnou stránku). Tento útok spočívá v napodobení oficiálních stránek stránkou podvodnou, kde je od uživatele vyžadováno zadání citlivých uživatelských údajů (jména, hesla, číslo karty a další.) [15]

Jedním typem obrany proti pharmingu je kontrola a ověřování URL adresy. Pharmingové útoky jsou založeny i na záměně písmenek v URL a odkáží vás tedy na jinou stejně vypadající webovou stránku, než je stránka oficiální. Dalším typem může být kontrola přítomnosti SSL certifikátu a kontrolovat vzhled stránky, zda není pochybný nebo rozdílný od stránky oficiální. [16]

Závěrem je tedy neotvírat pochybné odkazy na webové stránky, kontrolovat názvy odkazujících webových stránek a přítomnost zabezpečeného připojení (https://) a mít celkové povědomí, že tento druh útoku existuje a je třeba se proti němu těmito způsoby bránit.

5.2.4 Sniffing

Sniffing (čenichání, čmuchání) je metoda, která slouží k odchytávání elektronické komunikace v počítačové síti. Data odchytává prostředník mezi odesílatelem a adresátem dané komunikace.

---

[13] *Phishing a pharming* [online].
[14] Domain Name System – hierarchický systém doménových jmen, sloužící k překladu URL adres na IP
[15] BITTO, Ondřej. *Rhybaření střídá pharming* [online].
[16] PINKAVA, Jaroslav. *Phishing aneb rhybaření 1.* [online].

Tento útok je proveditelný pomocí sniffovacích programů (tzv. snifferů). Ty umožňují sledovat celou komunikaci, která prochází přes daný síťový uzel. Pomocí nich lze pak snadno vyčíst obsah komunikace včetně hesel a dalších citlivých údajů. Ukradená data mohou být dále použita k nezákonným průnikům nebo i psychickým útokům, především k vydírání.

Obrana proti sniffingu spočívá v dodržování základních pravidel, jimiž se pak snižuje riziko odposlouchávání. Naším cílem je tedy odeslat naše data tak, aby si je přečetla pouze osoba námi určená a nikdo jiný. K tomuto lze použít vhodné šifrování síťové komunikace např. pomocí SSL certifikátů, odesílání e-mailů podepsaných šifrovacím klíčem. Dále existuje spousta softwaru, které dokáží oskenovat počítač a odstranit nejrůznější typy škodlivých softwarů včetně snifferů. [17]

5.3 Sociální inženýrství

„Sociální inženýrství je ovlivňování a přesvědčování lidí s cílem oklamat je tak, aby uvěřili, že sociální inženýr je osoba s totožností, kterou předstírá a kterou si vytvořil pro potřeby manipulace.“ [18]

Sociální inženýrství tedy slouží k získání citlivých informací. Je založeno na vytvoření vztahu důvěry s vybranou obětí. Tato důvěra je samozřejmě ze strany útočníka falešná a jen „naoko“. Sociální inženýrství se snaží těžit z lidské důvěřivosti a snaze pomoci ostatním a právě těchto hodnot zneužívá ve svůj prospěch. Útoky bývají prováděny přímo, telefonicky nebo online. Většina technik je velmi jednoduchých, za to však velmi efektivních. Mezi oblíbené postupy patří vzbudit v lidech určitou zvědavost. Útočníci se snaží nabídnout speciální výhody nebo potenciální možnost výhry. Ve většině případů nepřijde útočník do osobního styku s obětí. Sociální inženýrství je nebezpečné, protože má vždy za cíl obelhat uživatele a získat určitý druh informací. [19]

Sociální inženýrství využívá mnoho triků a klamů. Mezi ně patří především:

Stres - lidé pod tlakem reagují jinak než lidé v klidu, kdy mají čas na přemýšlení. A tak jsou více zranitelní a udělají spoustu věcí bez přemýšlení, čehož pak mohou litovat.

[17] OBR, Jiří. *Sniffing: Odposlech datové komunikace* [online].
[18] Citace z: http://www.fi.muni.cz/usr/jkucera/pv109/2003p/xsimek3sociotechnika.htm
[19] KUNEŠ, Jakub. *Co je sociální inženýrství? - 1. díl* [online].

Důvěryhodnost - lidé mají tendenci věřit obecně lidem. Např. pokud přijde do prodejny technik s výbavou a řekne obsluze, že je objednán od vedoucí na opravu, nebude moc pochybovat o tom, že by lhal.

Vydávání se za někoho jiného - ptát se sám sebe, zda je osoba uvedena v e-mailu nebo po telefonu tím, za koho se vydává?

Zvědavost - například pokud někdo najde věc (třeba CD), která upoutá jeho pozornost a zvědavost vyhraje nad rozumem. Po vložení CD do mechaniky, spustí .exe soubor a místo kýženého obsahu si nainstaluje škodlivý nástroj.

Mezi techniky sociálního inženýrství patří například již výše zmíněný phishing (viz 4.2.2 Phishing), pharming (viz 4.2.3 Pharming) a dále pak Google Hacking.

5.3.1 Google hacking

Jak již z názvu vypovídá, Google hacking souvisí přímo s vyhledávačem Google. Každý z nás se jistě s vyhledávačem od Googlu setkal, ale málokdo ví, že je to vyhledávací prostředek i pro citlivé informace, které by měly zůstat skryté před cizími zraky. Údaje, které by měly být chráněné, jsou v mnoha případech dostupné. V podstatě stačí trocha trpělivosti a zadání správného vyhledávacího řetězce a mohou být napadena různá hesla nebo soukromé údaje konkrétních osob.

Google Hacking tedy spočívá v zadávání specifických operátorů do vyhledávání. Pomocí nich lze nalézt většinu důležitých informací. Používání operátorů vyžaduje alespoň základní znalost struktury stránky. [20]

Jedním ze základních operátorů je INURL, který umožňuje hledat přímo v adrese URL stránky. Takže na dotaz `inurl:digitalni stopy` vyhledávač vyhledá stránky, které mají slovo „digitální stopy“ přímo v URL adrese. Tento operátor se hodí především pro hledání určitých typů dat, která jsou uložena do speciálně pojmenovaných složek.

Dalším příkazem (operátorem) je INTITLE, který hledá text, který je zobrazen v titulku (horní části prohlížeče) stránky.

[20] MCCLURE, Stuart, Joel SCAMBRAY a George KURTZ. *Hacking exposed 7: Network Security Secrets and Solutions*. ISBN 978-0-07-178028-5.

Dalším užitečným parametrem může být příkaz FILETYPE, který nám umožní vyfiltrovat hledání na námi vybraný typ souboru. [21]

Google je velmi sofistikovaným vyhledávač, který o nás ví spoustu informací, o kterých my sami většinou ani nevíme. Příkladem toho může být Google Dashboard, který přehledně vypíše o přihlášeném Google uživateli všechna nashromážděná data o něm. V přehledu můžeme vidět například, kolik zařízení se systémem Android máme registrovaných v Google Play, dále pak kolik máme nainstalovaných aplikací z obchodu Play, kolik kontaktů máme uložených v kalendáři Googlu, jaké platby jsme platili přes službu Payments, kolik záložek máme uložených v Google Chrome a spoustu dalších věcí. Toto vše lze zjistit po přihlášení na https://www.google.com/settings/dashboard. Tato data naštěstí nejsou veřejně viditelná, takže je vidí pouze přihlášený uživatel a Google. [22]

Další zajímavostí je, že Google si o každém uživateli dělá takový svůj obrázek, jednak na základě námi navštěvovaných stránek, tak i podle informacích o nás na Google+. Na jejich základě se snaží odhadnout naše pohlaví, věk a zájmy a snaží se nám nabízet reklamy, které by nás mohly případně zajímat. Tento přehled si můžeme jednoduše zjistit pod následujícím odkazem: https://www.google.com/ads/preferences/. O dalších zajímavostech se lze dočíst na blogu Medium.com. [23]

6 Rizika digitálních stop

Zanechávání digitálních stop s sebou nese i určitá rizika. Prvním takovým rizikem může být krádež naší identity. Dalšími riziky pak kyberstalking nebo kyberšikana. Na závěr jsou popsány metody, jak se proti těmto rizikům účinně bránit.

6.1 Využití digitálních stop

Digitální stopy nacházejí využití především v personalistice, díky kterým si mohou personalisté sestavit obrázek o uchazečovi dříve, než při osobním setkání. Tyto informace obvykle získávají z aktivních digitálních stop, především tedy ze sociálních sítí.
Z rozhovoru s panem Bubeníkem a Novákem (zakladateli jednotlivých společností) vyplývá, že k hledání nových pracovníků hrají velkou roli sociální sítě, webová fóra a

[21] KRATOCHVÍL, Petr. *Google hacking: cíl zaměřen* [online].
[22] POLESNÝ, David. *Podívejte se, co všechno o vás ví Google* [online].
[23] *6 links that will show you what Google knows about you* [online].

blogy. Díky digitální stopě se HR [24] manažeři a personalisté dozvídají o potenciálních uchazečích i informace a reakce chování, které by byly dle životopisu nezjistitelné a zjistily by se třeba až na osobním pohovoru. Pan Bubeník tvrdí, že by personalisté měli jít za lidmi tam, kde se pohybují (chatovací fóra, blogy). Milan Novák v rozhovoru říká, že je zásadní si uvědomit, že naši digitální stopu nelze vymazat. Vše, co se na sociálních sítích objeví, tam zůstane. Pro zaměstnavatele může být důležité, jak se kandidát choval v historii, jaké názory sdílel atp. V závěru rozhovoru říká: *„Každý z nás tu digitální stopu už vytváří nebo začíná vytvářet. Proto bychom pokaždé, než nějaký obsah vložíme na danou sociální síť, měli dobře zvážit, zda nás to v budoucnu nemůže nějak poškodit.“* [25]

Personalisté mohou dále pátrat po informacích, které by mohly ovlivnit uchazečovo přijetí do společnosti. Typickým příkladem mohou být nevhodné fotky a vulgární komentáře potenciálního zaměstnance.

Z článku Olivera Perkinse z března 2015 vyplývá, že až 52% personalistů používá sociální sítě k hledání kandidátů. Kandidáti, kteří tvrdí, že se nemusí čeho bát, že nejsou na sociálních sítích, ovšem nemají tak úplně pravdu. Ze statistik dále vyplývá, že až 35% personalistů osloví méně raději kandidáty bez digitální stopy, než kandidáty se stopou. [26]

Uživatelé na tyto věci reagují tím, že si omezují viditelnost a přístup k některým jejich informacím. I přesto jsou známy případy, kdy zaměstnavatel požadoval po uchazeči během pohovoru přístup k jejich údajům na sociálních sítích. Osobně si myslím, že na toto nemá zaměstnavatel žádné právo, protože může dojít k vážnému porušení soukromí a možnému zneužití informací o dané osobě.

Závěrem bych řekl, že by se uživatelé měli na internetu chovat a jednat tak, jak jednají ve skutečnosti. Každý by si měl uvědomit, že na internetu by měl být pouze „obraz“ jejich reálné identity. Spousta lidí si toto postupem času uvědomuje a snaží se mít svoji digitální stopu „pod kontrolou“.

[24] Human resource - lidské zdroje
[25] CHLUPATÝ, Roman. *Digitální stopa: Jak si nezavřít cestu k práci snů? Využívejte sociální sítě s rozumem, radí experti* [online].
[26] PERKINS, Olivera. *More than half of employers now use social media to screen job candidates, poll says; even send friend requests* [online].

6.2 Krádež identity

S krádeží identity úzce souvisí již řečený pojem Osobní údaj. S krádeží identity se můžeme setkat ve dvou prostorech. V prvním případě jde o reálné prostředí, kdy dojde nejčastěji k odcizení osobních údajů člověka. Poté se zloději mohou pohybovat pod cizím pasem, občanským průkazem a uzavírat půjčky a smlouvy na tuto okradenou osobu. Hlavním důvodem je ve většině případů finanční zisk nebo poškození reputace dané osoby.

V druhém případě jde o prostředí internetu. Zde dochází k odcizení častěji a snáze, protože neexistují fyzické hmatatelné podklady, takže je těžší si všimnout odcizení. Útoky jsou prováděny v největší míře za pomocí phishingu (viz Phishing), kdy se od uživatele útočníci snaží získat zejména: číslo platební karty, bezpečnostní kód platební karty (CVV), hesla, aktivní e-mailové adresy, rodné číslo, datum narození atd. Další metodou pro krádež identity je i zmíněný Google Hacking, za pomocí kterého lze vyhledat citlivé údaje o uživatelích. [27]

Výzkum společnosti Mediacom v roce 2014 odhalil, že 3 ze 4 Čechů dostali podvodný e-mail, který je vyzýval k uhrazení falešného dluhu nebo k instalaci škodlivého programu. Zcizení online identity přiznalo 13 % dotázaných. 80% dotázaných respondentů se obává odcizení jejich identity, virů a podvodných mailů. Většina těchto lidí neví, jak se proti těmto hrozbám účinně bránit. Z průzkumu dále vyplývá, že více jak polovina uživatelů nemá zabezpečené jejich mobily a tablety antivirovými programy. Přičemž třetina uživatelů využívá mobil a tablet pro internetové bankovnictví. [28]

Jiří Palyza z Národního centra bezpečnějšího internetu tvrdí, že pokud se lidé nebudou aktivně bránit proti kyberzločinnosti, počet kyber krádeží identity velmi rychle poroste.

Nejlepší obranou proti krádeži identity je používat zdravý selský rozum v kombinaci s antivirovým programem. Znát danou problematiku a rizika a dbát na obezřetnost a prevenci.

[27] NYKODÝMOVÁ, Helena. *Bojíte se krádeže své identity?* [online].
[28] *Digitální vydírání a krádež identity hrozí polovině populace* [online].

Obrázek 2 - Kyberútoky na mobilní zařízení (zdroj: APOGEO Esteem)

6.3 Kyberstalking

Pojem kyberstalking je speciální případ stalkingu, který se na rozdíl od něj neodehrává v reálném životě, ale na internetu. Kyberstalking tedy využívá moderní informační technologie a komunikace k vydírání a obtěžování obětí. Stalking je způsob chování, kdy se agresor zaměří na konkrétní osobu a tu pak pronásleduje. Útočník oběť obtěžuje a v některých případech jí může hrozit i fyzickým napadením. Při běžném stalkingu útočník oběť zasypává sms zprávami, telefonáty nebo dárky, o které nemá oběť zájem. U kyberstalkingu jsou oběti zasílány zprávy pomocí instant messengerů, e-mailů, chatu a pomocí sociálních sítí. [29]

Jelikož na sociálních sítích lze o jednotlivých uživatelích najít spoustu údajů (zvláště, pokud je mají veřejné), není tak pro stalkery problém, počkat si na ně před školou nebo přímo před jejich domem. Spousta uživatelů má dále veřejný e-mail, který mohou stalkeři také efektivně využít.

Kyberstalking může dále vést k poškození pověsti napadené osoby, může dále rozšiřovat nepravé informace mezi její známé a přátele. Útočník může například vytvořit nepravý profil oběti a udávat nepravé informace o osobě. Všechno toto velmi působí na psychiku člověka.

[29] ECKERTOVÁ, Lenka a Daniel DOČEKAL. *Bezpečnost dětí na internetu: rádce zodpovědného rodiče: Network Security Secrets and Solutions*. s. 67. ISBN 978-80-251-3804-5.

Kybestalking můžeme dělit na přímý a nepřímý:

- Přímý kyberstalking - využití mobilních telefonů a e-mailu pro odesílání zpráv
- Nepřímý kyberstalking - používání internetu k zobrazení zpráv a k šíření nepravých informací

V České republice nebyl stalking do roku 2010 právně postihnutelný. Od roku 2010 došlo k zavedení nového trestného činu tzv. stalkingu.

Organizace Working to Halt Online Abuse, která se zabývá bojem proti online obtěžování, udělala statistiku týkající se kyberstalkingu v letech 2000 - 2011. Z průměrných statistik všech let vyplývá, že oběťmi byly téměř ze 75 % ženy. Útočníky byli z 48 % muži a z 30 % ženy. Dalším aspektem je, že oběti byli nejvíce osoby mezi 18 až 30 lety. Nejčastějším prostředkem pro obtěžování byl e-mail a to ve 35 % případech. [30]

Jedním z poměrně nedávných případů kyberstalkingu je žena s falešnou identitou, která vylákala od muže 25 tisíc korun. Žena zveřejnila na internetovou seznamku fotku cizí osoby, za kterou se vydávala. S mužem navázala kontakt a několikrát si vzájemně volali. K jejich setkání však nedošlo, protože žena schůzku na poslední chvíli zrušila. Žena poté požadovala proplacení hovorů s mužem a ten jí je proplatil. Na další proplácení peněz však již muž nepřistoupil a falešná podvodnice mu začala volat z různých telefonních čísel a psát z e-mailů. Vulgárně ho urážela, budila ho ze spaní, obtěžovala ho v pracovní době. [31]

Obranou proti kyberstalkingu je založena především na nesdělování informací (bydliště, názvu školy, e-mailové adresy atp.) Věnovat pozornost bezpečnosti na sociálních sítích, zabezpečení našeho profilu a nemít informace viditelné veřejně.

6.4 Kyberšikana

Pojem kyberšikana úzce souvisí s již řečeným kyberstalkingem. Jedná se o šikanu, při které je zapotřebí informační a komunikační technologie (především internet, telefon). Šikana a kyberšikana mají jedno společné a to ublížit, ohrozit nebo zastrašit vybranou osobu nebo skupinu osob. Kyberšikana se oproti normální šikaně šíří mnohem rychleji a je

[30] HALTABUSE.ORG. *Comparison Statistics 2000-2011* [online].
[31] HORÁČEK, Aleš. *Nikdy ji neviděl, žena z inzerátu ho i tak zavalila sprostými esemeskami* [online].

dlouhodobá. Také ji lze velmi těžko zastavit, protože virtuální útočníci jsou téměř nedohledatelní. [32]

Kyberšikana může mít mnoho forem:

Obtěžování - útočník zasílá opakovaně kruté, bolestivé zprávy oběti nebo při krádeži hesla i přátelům oběti

Ponižování - pachatel šíří lži a pomluvy o oběti, snaží se poškodit její pověst mezi ostatními, může vytvářet i stránky a obrázky zaměřené na urážení a vysmívání se vybrané oběti

Sdílení - útočník má k dispozici určitá tajemství nebo fotky osoby, které pak záměrně šíří bez souhlasu oběti mezi ostatní uživatele (kamarády)

Flaming - útočník se snaží neustále hádat, vyvolává hádky, uráží a ponižuje oběť

Kyberšikana má oproti normální šikaně několik výhod. Zde je seznam některých z nich:

- Útočník bývá zpravidla anonymní a špatně zjistitelný
- Útočník může působit prakticky odkudkoli a kdykoli, stačí mu připojení k internetu
- Útočník může jednat mnohem agresivněji, než by jednal v realitě
- Obětí může být díky anonymitě kdokoli, třeba i učitel, kterého šikanuje žák [33]

Deník.cz vydal článek s titulkem „Každé třetí dítě v Česku má zkušenosti s kyberšikanou“. Ředitel Úřadu pro mezinárodněprávní ochranu dětí Zdeněk Kapitán v článku tvrdí, že případů kyberšikany je daleko více, ale odhalit se jich podaří jen zlomek. Podle něj je třeba, aby rodiče měli kontrolu nad dětmi, jejich pohybu na internetu, a kontrolu nad tím, s kým si jejich děti píší. „ Rodič nemusí detailně dítěti kontrolovat počítač, stačí jen, aby jej o věci poučil, uvedl Kapitán. „Již jen pouhé vědomí toho, že rodič si věci může zkontrolovat, může být dostatečnou prevencí," dodal ředitel. [34]

Případy kyberšikany je dobré nahlásit administrátorovi, rodičům nebo učitelům, v nejzávažnějších případech na policii. Obrana proti kyberšikaně je obdobná jako proti kyberstalkingu, tedy prevence, prověřování a nesdělování citlivých informací.

[32] *Kyberšikana* [online].
[33] JELÍNEK, Lukáš. *(NE) Bezpečný Internet* [online].
[34] ČTK. *Přibližně každé třetí dítě v Česku má zkušenost s kyberšikanou* [online].

6.5 Kybergrooming

„Kybergrooming je psychická manipulace prostřednictvím moderních komunikačních technologií s cílem získat důvěru oběti, vylákat ji na osobní schůzku a zpravidla sexuálně zneužít.“ [35]

Kybergrooming je poměrně zákeřný způsob, jak využít lidské důvěřivosti, touhy po přátelství a naivity. Pachatel si důvěru vytipované osoby získává pomalu a postupně v delším časovém období. Největší ohroženou skupinou jsou děti a mladiství do 18 let. Jako kybergroomera tedy můžeme definovat útočníka, který pro získání oběti využívá informačních a komunikačních prostředků. Často také vystupují pod falešnou identitou.

Průběh budování závislosti oběti na kybergroomrovi:

1. Vzbuzení důvěry
2. Kupování dárků, podplácení
3. Získávání materiálů k vydírání
4. Emociální závislost na kybergroomovi
5. Osobní setkání
6. Zneužití, vydírání [36]

Nejznámějším příkladem kybergroomingu v České republice je kauza Pavla Hovorky. Ten navazoval pomocí internetu komunikaci s nezletilými dětmi. Nejdříve si u dětí vybudoval postupnou důvěru a poté si děti začal vodit k sobě domů, kde je zneužíval. Byl obviněn za zneužití 21 dětí a odsouzen na 8 let vězení. [37]

Jak se tedy bránit kybergroomingu? Nejlepší obranou je opět prevence, která spočívá v dobré komunikaci mezi rodiči a dětmi. Rodiče by měli být informováni o činnostech svých dětí a dítě by k nim mělo mít důvěru a svěřovat se jim. Dalšími obranami může být například nesdělování osobních informací (zvláště neposílat intimní osobní fotky), všímat si nesrovnalostí v komunikaci s kybergroomery, nenechat se oklamat nebo zlákat na odměny za fotky atp.

---

[35] Citace z: *Kybergrooming a Kyberstalking: Metodický materiál pro pedagogické pracovníky* [online]. s. 4
[36] *Kybergrooming* [online].
[37] NEJEZCHLEBOVÁ, Lenka. *I mě zneužil deviant Hovorka. Ten ksicht nezapomenu, vzpomíná žena*[online].

7 Kontrola naší digitální stopy

V následující části se bakalářská práce zaměří na konkrétní metody pro zjištění zanechaných digitálních stop, nejdříve aktivních poté pasivních.

7.1 Aktivní

V tomto případě se jedná o námi vědomě zanechané informace o nás (viz Aktivní digitální stopy).

Pro kontrolu našich aktivních digitálních stop poslouží velmi dobře tzv. „egosurfing“ nebo také „egogoogling“. Tento proces je velmi jednoduchým a efektivním způsobem, jak si ověřit aktivní digitální stopu jednotlivých osob. K egosurfingu nám postačí jakýkoli internetový vyhledávač a jeho princip spočívá v zadání osobních informací o námi ověřované osobě jako je jméno, příjmení, ale i přezdívka, místo bydliště atp. Tímto způsobem si můžeme udělat obrázek i o lidech, které jsme nikdy v reálu neviděli. Toho využívají především personalisté, kteří využívají egosurfingu nejvíce. Zjišťují si tak předem informace o uchazečích o danou práci.

V souvislosti s egosurfingem vzniklo i několik specializovaných vyhledávačů (People search engines), které se zaměřují pouze na vyhledávání digitálních stop. Rozdílem oproti běžným vyhledávačům a takto specializovaným je především v zobrazení výsledků informací o hledaných osobách. U specializovaných vyhledávačů se zobrazí celkový seznam nalezených informací, nikoli jen hypertextové odkazy.

7.1.1 People search engines

People search engines jsou tedy alternativou ke klasickým vyhledávačům. Oproti nim umožňují třídit vyhledané informace podle kategorií a obsahují i funkce, které umožňují zvýšit i počet informací. Stránka http://www.ebizmba.com/articles/people-search obsahuje aktuální přehled nejvyužívanějších people search enginů.

7.1.1.1 Pipl

Jako jeden z příkladů jsem si vybral Pipl, který je jedním z nejznámějších a nejpoužívanějších people search enginů. Pipl je zcela zdarma a umožňuje vyhledávat uživatele podle jména, e-mailu, přezdívky, tel. čísla a bydliště. [38]

7.1.1.2 Spokeo

Spokeo je dalším známým people search enginem, který po zadání údajů prohledává všechny známé sociální sítě. Je velmi komplexní, ale pro zobrazení výsledků je třeba být registrován a platit členství.

Dalšími stránkami pro vyhledávání mohou být např. People finders (obsahuje i databázi s kriminálními záznamy, ovšem jen pro USA), 192, či Whitepages.

Za zmínku stojí také stránka Skipease [39], která sdružuje mnoho známých People Search enginů.

7.1.2 Google Dashboard

Jak již bylo uvedeno výše, Google Dashboard je nástroj, kterým můžeme spravovat naší online identitu. Jedná se především o služby, které spadají pod Google (Gmail, Google+, Youtube, Google kalendář atd.).

Toto vše lze spravovat z jednoho jediného místa. Nalezneme zde přehled o námi využívaných službách a námi poskytovaných informací. Krom toho zde lze upravovat soukromí u jednotlivých služeb včetně možností úplného odstranění informací.

7.1.3 Google Alerts

Google Alerts (též Me on the web) je užitečná služba Googlu, která umožňuje sledovat a upozorňovat uživatele na novinky, o které se uživatel zajímá. Jedná se tedy o monitorovací službu. Stačí zadat do vyhledávání námi vybraný výraz a postupně nám začnou chodit do G-mailu odkazy na webové stránky, kde se tento výraz objeví.

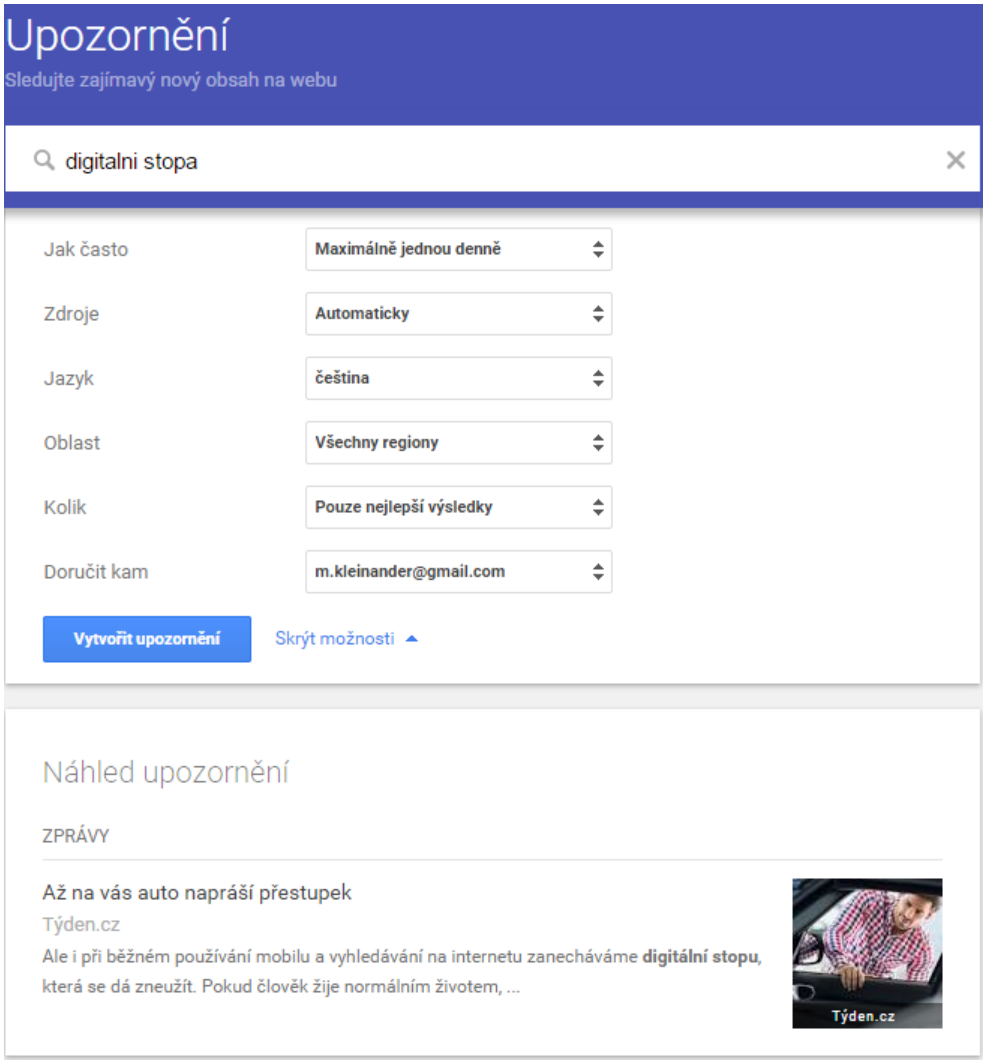
Pro používání je třeba mít vytvořený účet u Googlu a jít na stránku: https://www.google.com/alerts

---

[38] Centre for the Protection of National Infrastructure. *Tracking my digital footprint: A guide to digital footprint discovery and management* [online].
[39] *Skipease: The Best People Search Engines* [online].

Poté již stačí zadat do vyhledávání daný výraz a na stavit u něj parametry. Jako parametry můžeme nastavit například zdroje, četnost zasílání oznámení, jazyk a místo doručení oznámení. [40]

Tyto upozornění můžeme využít právě v souvislosti s kontrolou naší digitální stopy a to především, pokud do upozornění zadáme naše osobní údaje (např. jméno a příjmení, přezdívky, e-mailové adresy atd.). V tomto případě, pokud se naše údaje objeví na nějaké webové stránce, bude nám zasláno oznámení o této události. Lze také nastavit frekvence zasílání těchto upozornění. [41]



Obrázek 3 - Příklad vytvoření Google Alertu (zdroj: vlastní archiv autora)

[40] ŠIMEČEK, Martin. *Google Alerts* [online].
[41] BLIZCO, Marek. *Upozornění Google (Google Alerts) nyní k dispozici v češtině a slovenštině* [online].

7.1.4 Facebook - stáhnutí informací

Nejznámější sociální síť Facebook nabízí uživatelům mimo jiné i stažení archivu se záznamy, které o sobě uživatel zanechal na sociální sítí. Spousta uživatelů ani neví, že tuto funkci Facebook vůbec nabízí. Tento archiv obsahuje jak aktivní, tak pasivní digitální stopu uživatele.[42]

Aktivní digitální stopu tvoří zvláště uživatelem vyplněné informace, jako jsou např. kontaktní údaje, komentáře a příspěvky, nahrané fotky a videa, seznam přátel, přijaté a odeslané zprávy apod. Jedná se tedy o kopii uživatelova profilu.

Pasivní digitální stopu tvoří zajímavější informace s větší vypovídací hodnotou. Nalezneme zde například seznam IP adres, ze kterých bylo připojováno k účtu, dále názvy zařízení a prohlížeče, přes které došlo k připojení, přijaté cookies, dále zde nalezneme nastavení soukromí a viditelnost sdělovaných informací, změny stavu účtu (aktivace, deaktivace).[43]

Tento nástroj je užitečný pro aktuální přehled o našem účtu a jeho nastavení. Bohužel ale nezobrazuje položky, které uživatel během doby trvání účtu smazal. Tato data tak nejsou pro běžného uživatele viditelná, ačkoli má Facebook tato smazaná data stále uložena na serverech. Z výzkumu vyplývá, že archiv obsahuje přibližně třetinu informací, které Facebook o uživatelích shromažďuje.

Jak vyplývá z článku na magazínu Facemag.cz, Facebook sleduje spoustu věcí o kterých ani nevíme. Jednou z nich je to, že zachycuje i příspěvky a komentáře, které jsme napsali, ale poté je smazali a tedy ani nepublikovali. Tento nashromážděný text byl následně analyzován a data byla posílána zpět do serverů Facebooku. Facebook jasně uvádí, že shromažďuje pouze informace, které chtějí uživatelé sdílet. Bohužel ale shromažďuje i to, co uživatelé nesdílejí, aniž by si toho byli uživatelé vědomi.[44]

[42] *Facebook: Stahování informací o vás* [online].
[43] KOTENKO, Jam. *Want to know what data Facebook has on you? A primer on what you get and how to get it* [online].
[44] FACEMAG.CZ. *Facebook si čte i to, co nechcete sdílet* [online].

7.2 Pasivní

U pasivních stop je šance na odhalení a jejich kontrolu poměrně malá, oproti aktivním stopám. Hlavním důvodem je, že běžní uživatelé si stále neuvědomují jejich sledování třetími stranami, které uchovávají informace o uživatelích ve svých databázích. Neznají danou problematiku a nepovažují je za riziko ohrožení soukromí. Jedná se především o zadané osobní údaje při nákupech přes e-shopy a registracích. Uživatelé jsou tedy nuceni ve většině případů zanechat po sobě určité informace na jistých webových stránkách.

Tyto informace jsou v dnešní době velmi cenné a velmi často se s nimi i obchoduje. Díky těmto obchodům je pro uživatele prakticky nemožné zjistit, kam až se jeho osobní údaje dostaly. Často se tak stává, že firmy získají uživatelovo telefonní číslo či e-mail a začnou mu posílat nevyžádanou poštu či mu dokonce volat, aniž by se u této společnosti v minulosti registroval, či elektronicky nakupoval.

7.2.1 Google Ad Preferences

Nástroj od společnosti Google, který umožňuje uživatelům upravovat informace, kterých je využíváno při doručování cílených reklam na jednotlivé uživatele. Je známo, že společnost Google sleduje aktivity uživatelů a na základě nich pak sestavuje tuto cílenou reklamu na míru uživatelů. Toto cílení probíhá především na základě zadaných klíčových slov do vyhledávání, shlédnutých videí na Youtube a na základě uživatelova pohlaví a věkové skupiny. Po přihlášení do účtu Googlu má uživatel na odkazu https://www.google.com/settings/u/0/ads/authenticated možnost si nastavit zobrazení reklam, které ho zajímají. Dále má uživatel možnost tuto cílenou reklamu od Googlu úplně zakázat. [45]

Jak vyplývá z článku na Technetu: "Google prochází všechny vaše e-maily a hledá v nich klíčová slova, aby vám mohl zobrazit na vás zacílené reklamy," varuje Microsoft při své kampani, kdy se snaží oslabit popularitu Gmailu a přenést uživatele na jejich Outlook.com. Microsoft v článku poukazuje především na zásah Googlu do soukromí uživatelů, kdy Google pomocí algoritmu prohledává klíčová slova v uživatelských e-mailech a na základě nich pak sestavuje cílenou reklamu. [46] Tento nástroj neumožňuje uživatelům zjistit

[45] KYLIÁN, Ivo. *Jak vypnout vtíravé zobrazování určitých reklam Google?* [online].
[46] KASÍK, Pavel. *Microsoft: Pozor, Google čte vaše osobní maily, pojďte radši k nám* [online].

komplexní rozsah jejich pasivní digitální stopy. Slouží spíše k sestavení přehledu uživatelova profilu reklamními společnostmi. Uživatelé tedy vidí, co si o nich Google myslí na základě jejich dotazů zadaných ve vyhledávání a jejich chování na internetu.

8 Správa digitálních stop

8.1 Aktivních

U aktivních digitálních stop je nejpodstatnější si uvědomit, jaké informace a data o sobě vypustíme do světa internetu. Jakmile se tam jednou tyto informace o nás dostanou, je velmi obtížné až skoro nemožné je odstranit. Nejlepší ochranou je tedy prevence a střízlivost ve sdělování informací. Pokud uživatel bude chtít o sobě sdílet určitě informace, je třeba dbát určitých bezpečnostních zásad. [47]

Těchto zásad a pravidel je poměrně mnoho. Uvedu zde jen nejzákladnější (o některých z nich jsem se již zmínil v Kapitole 5). [48]

- Nastavení soukromí u služeb, především u sociálních sítí. To umožňuje omezit viditelnost uživatelových citlivých informací cizím osobám. [49]
- Používat více přihlašovacích jmen, e-mailů a hesel pro různé služby. To vše ztěžuje získání informací o uživateli a jeho identifikaci. Zároveň dochází i k většímu zabezpečení uživatelských účtů v případě prolomení hesla a dalších citlivých údajů (viz 5.2 Krádež identity)
- Nastavení zabezpečení prohlížeče. a to především správa cookie souborů (viz Kapitola 3.1 Cookies). Každý moderní prohlížeč nabízí správu cookie souborů, jejich prostřednictvím lze blokovat přijímání cookies (především 3rd party cookies) či nastavovat výjimky pro určité servery. V poslední řadě je důležité kontrolovat a mazat již uložené cookie soubory pro případ, že by došlo k jejich zneužití. Především tehdy, když by útočník získal přístup k počítači uživatele (veřejné kavárny, knihovny apod.), neboť cookies na počítači nejsou nijak chráněny.

[47] ZADRAŽILOVÁ, Iva. *Nebezpečí zneužití osobních informací v době globálního monitoringu s přihlédnutím k možnostem ochrany soukromí. Část II.* [online].
[48] TECHCENTRAL. *Digital Footprints* [online].
[49] Centre for the Protection of National Infrastructure. *Tracking my digital footprint: A guide to digital footprint discovery and management* [online].

- Střídmé publikování fotek, videí, příspěvků v prostředí internetu, hlavně na sociálních sítích a diskuzních fórech. Uživatelé by si měli přečíst podmínky pro užívání dané služby a podmínky o zpracování osobních údajů a vyjádřit souhlas či nesouhlas s těmito podmínkami. Dále by měl být uživatel obeznámen, jak bude s jeho informacemi dále nakládáno. [50]

Pro správu aktivních digitálních stop je ideálním nástrojem již zmíněný Google Alerts (viz 6.1.3 Google Alerts), který umožňuje uživatelům pravidelné vyhledávání a zasílání jimi zadaných klíčových výrazů (aktivních stop) v podobě upozornění.

8.2 Pasivních

Pohyb uživatelů v prostředí internetu je bez zanechání pasivní digitální stopy téměř nemožný. Jsou však způsoby, díky kterým mohou uživatelé chránit své soukromí před riziky souvisejícími s pasivními digitálními stopami (zvláště sledování chování uživatelů). Pro tyto účely byly vyvinuty nástroje, které tuto problematiku řeší.

8.2.1 Opt-out

Pojem opt-out je obecně způsob, jakým se mohou uživatelé zbavit nechtěné služby. V souvislosti s informačními technologiemi se může jednat například o zrušení zasílání nabídek prostřednictvím e-mailu. Uživatel klikne na odkaz uvedený v e-mailu odesílatele a zašle požadavek na zrušení posílání dalších nabídek. Opt-out nabízí velká část reklamních společností a slouží ke zrušení reklamy cílené na základě chování uživatelů.

Princip Opt-outu je založen na uložení informací prostřednictvím souboru cookies na náš disk. Ten poté serveru sdělí, že si uživatel nepřeje cílenou reklamu. Tuto cookie je třeba v počítači chránit, protože pokud by došlo k jejímu odstranění, uživatel by byl opět cílen behaviorální reklamou. [51]

V rámci společnosti Googlu a jeho služeb se může uživatel vyvázat z cíleného reklamy prostřednictvím zmíněného Google Dashboardu, kde si může toto sledování a cílenou reklamu zrušit. [52]

[50] ČERNÝ, Michal. *Digitální stopy* [online].
[51] KRATOCHVÍL, Petr. *Vaše stopy na internetu* [online].
[52] Google. *Opt out* [online].

8.2.2 Anonymní prohlížení

Anonymizační techniky jsou další možností, jak po sobě zanechat méně informací v prostředí internetu. Tyto nástroje umožňují skrýt nebo změnit údaje (IP adresu, http hlavičky), které lze využít k identifikaci zařízení. Anonymizačních prostředků je velmi mnoho a liší se především mírou zabezpečení, použitou technikou, dostupností. Zaměřím se však pouze na volně dostupné nástroje

8.2.2.1 Anonymní módy

Základní a nejjednodušší cestou, jak získat částečnou anonymitu je použití anonymních režimů v prohlížečích. Touto funkcí v dnešní době disponují známé prohlížeče. U Internet Exploreru a Edge je to InPrivate browsing, Opera, Mozilla a Safari mají Private browsing, Google Chrome Incognito mode. Tyto módy mají téměř totožné funkce a jejich hlavním úkolem je zabránit ukládání historii procházení webových stránek, historii stahovaných souborů, některá rozšíření (pluginy) a po ukončení prohlížení v anonymním režimu dochází ke smazání přijatých cookies a historie procházení. [53]

Největším rizikem z hlediska bezpečnosti jednotlivých prohlížečů jsou jejich doplňky a zásuvné moduly, které slouží k rozšíření funkčnosti prohlížečů. Tyto doplňky a moduly jsou primárně povoleny v běžném režimu, avšak u některých prohlížečů např. Mozilly Firefox běží tato rozšíření i v anonymním režimu bez možnosti je zakázat. Což vede ke stálému sledování uživatelových aktivit, i když je v „bezpečnějším“ prohlížecím režimu. Oproti tomu Google Chrome a IE mají tyto doplňky při spuštění anonymního režimu primárně zakázané, lze je však v případě potřeby ručně zapnout v nastavení prohlížeče. [54]

8.2.2.2 Webové proxy

Proxy server je zařízení (server, router), které má přidělenou veřejnou IP adresu a tvoří prostředníka při komunikaci klienta se serverem. Odděluje tak lokální počítačovou síť od Internetu. IP adresa uživatele je skryta za IP adresu proxy serveru. Nejlepší a nejjednodušší přístup k proxy serverům nabízejí volně dostupné webové anonymizéry, neboli webové proxy servery. Jedná se o webovou stránku s vyhledávacím oknem podobné napr. Googlu. Do vyhledávání stačí vložit požadovanou URL adresu stránky a proxy server ji poté načte.

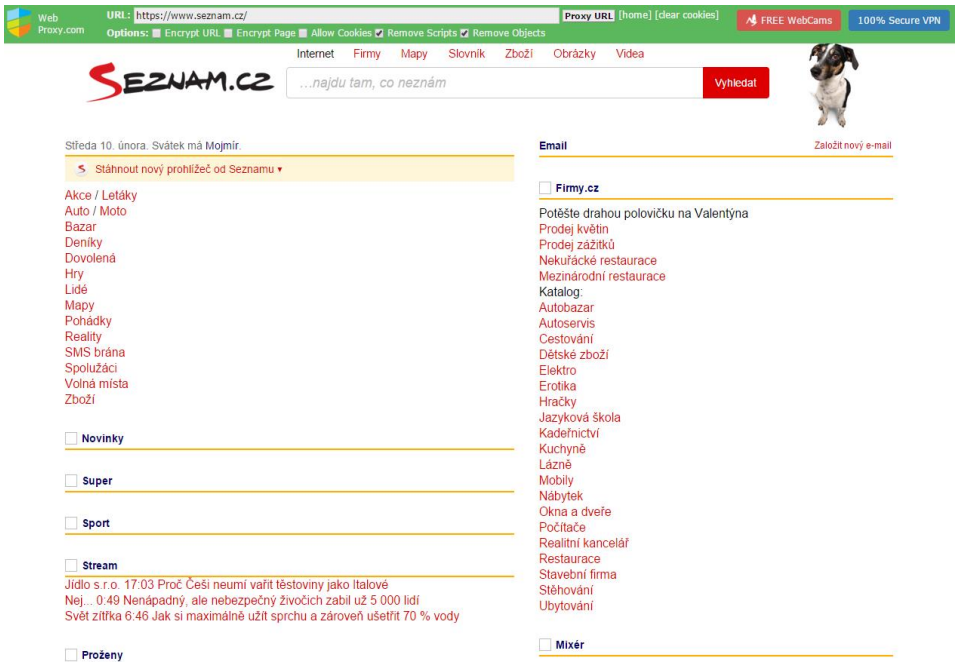
[53] ŠÍMA, Josef. *Anonymní prohlížení* [online].
[54] KRATOCHVÍL, Petr. *Anonymní surfování* [online].

Dále lze před zadáním textového řetězce zvolit mnoho parametrů, např. zda mají být povoleny cookies, zakázány skripty pro rychlejší načtení stránek, zda mají být odebrány Java a Flash objekty a mnoho dalších.

V praxi existuje mnoho proxy serverů. Důkazem toho je stránka http://proxy.org/web_proxies.shtml, kde je velký seznam nejrůznějších proxy serverů. Liší se od sebe především dostupností a funkcemi. Důležitou roli ve výběru proxy serveru hraje jeho umístění v závislosti na naší poloze, od které se odvíjí doba odezvy serveru.

Jednoduchost řešení za pomocí proxy serveru s sebou nese však i několik nevýhod. První z nich zpravidla malá rychlost přenosu dat (pokud je server velmi daleko od nás). [55] Dalším problémem je, že ne všechny anonymizéry blokují http hlavičky, které pak mohou prozradit uživatelovu IP adresu. Posledním velmi zásadním problémem je důvěryhodnost proxy serverů, protože spousta z nich může být napadena virem nebo být ovládána hackerem.

Pro demonstraci jsem si vybral známý volně dostupný proxy server Webproxy.com [56] na kterém jsem použil URL adresu Seznamu.cz a zvolil parametry: Nepovolovat cookies, odebrat skripty a objekty (viz obrázek 4).



Obrázek 4 - Použití proxy serveru Webproxy.com (zdroj: vlastní archiv autora)

[55] KREUZIGER, Pavel a Brad CHACOS. *Jak (a proč) surfovat na webu v utajení - 2. díl* [online].
[56] *Webproxy* [online].

8.2.2.3 Vícenásobné proxy

Lepší ochranu než webové proxy nabízejí nástroje, které využívají modelu klient - server s tím, že se datové pakety přenášejí přes několik uzlů (routerů). To zajišťuje těžkou identifikaci uživatele a umožňuje tak velmi vysokou anonymitu. Jako nejznámější zástupce bych uvedl nástroj Tor a I2P.

8.2.2.4 Tor

Tor je nástroj, který zajišťuje anonymizaci v prostředí Internetu za pomoci anonymních proxy serverů. Jedná se o zkratku The Onion Routing, což v doslovném překladu znamená "cibulové směrování". Tento princip spočívá v cestování datových paketů přes mnoho Tor routerů. Cibulové směrování proto, že každý datový blok se skládá z vrstev, kdy každá z vrstev je šifrována jiným klíčem a nese s sebou informaci, na jaký Tor router se má dále poslat. Jakmile data dorazí na další router, dojde k dekódování (odstranění svrchní vrstvy) a cyklus se opakuje do té doby, než dojde k poslání paketů na cílový router. Cíl si tedy bude myslet, že ve skutečnosti komunikuje s posledním routerem, který mu zaslal data. Dojde ke zpracování požadavku a pošle odpověď zpět přes síť Tor routerů, kde dojde opět k "obalení" do vrstev a šifrování. Tím je původní zařízení, které vyslalo dotaz, velmi těžké identifikovat. [57]

Jednotlivé Tor routery představují zpravidla počítače dobrovolníků, kteří si nastavili Tor klienta jako veřejný uzel, přes který mohou putovat pakety dále.

Jednou z nevýhod souvisejících s onion routingem je právě rychlost přenosu dat, která závisí na každém jednotlivém uzlu (dobrovolníkovi). V praxi je rychlost přenosu dat srovnatelná s vytáčeným připojením a webové stránky se tak načítají v řádu minut.

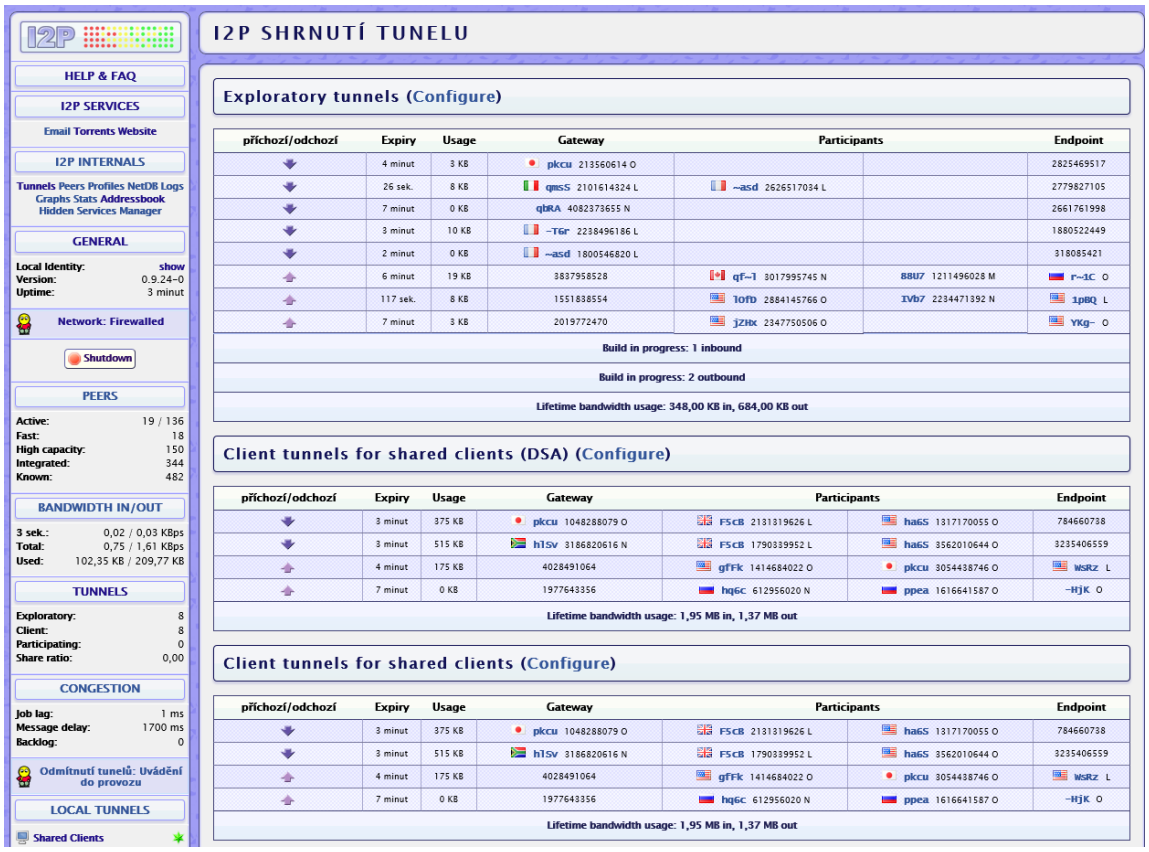
Do Toru lze přistupovat různými způsoby. Jedním z nich je pomocí klienta a proxy serveru, který lze stáhnout z oficiálních stránek projektu Tor. Dalším řešením jsou webový klienti podporující Tor, např. OperaTor (upravený prohlížeč Opera) či xB Browser (upravený Mozilla Firefox). Webový klienti jsou nejjednodušším a nejpraktičtějším řešením.[58]

[57] ČMELÍK, Martin. *TOR (The Onion Router) - systém pro vysoce anonymní a šifrovaný přístup k Internetu*[online].
[58] ČÍŽEK, Jakub. *TOR: Skutečně anonymní internet* [online].

8.2.2.5 I2P

Nástroj I2P (Invisible Internet Project) je decentralizovaná síť velmi podobná Toru. Tato síť je provozována především dobrovolníky po celém světě a její princip spočívá v P2P vzájemné komunikaci klientů, kdy jednotlivé routery uživatelů posílají své požadavky prostřednictvím tzv. "tunelů". Když tedy chce klient poslat zprávu dalšímu klientu, dochází k poslání této informace z koncového tunelu na vybraný cílový počáteční konec dalšího klienta. I2P slouží jako brána do alternativního "internetu" tzv. Darknetu[59]. Síť má adresy se speciální koncovkou .i2p, které na běžném internetu nelze zobrazit. Je tedy třeba nainstalovat router I2P a nastavit proxy server, který tyto adresy a I2P internet zpřístupní.[60]

I2P obsahuje oproti Toru mnoho dalších služeb jako například instant messaging, poštovní systém, UDP komunikaci a další. Bohužel je ale méně populární a využívaný. Proto je nedostatek routerů a surfování je tak velmi pomalé.



Obrázek 5 - klient I2P s přehledem jednotlivých tunelů (zdroj: vlastní archiv autora)

[59] Darknet je síť, do které lze přistupovat pouze pomocí speciálního softwaru a konfigurace
[60] *The Invisible Internet Project (I2P)* [online].

8.3 Možnost odstranění digitálních stop

Možností, jak odstranit naše digitální stopy je poměrně mnoho, ale je prakticky nemožné 100 % odstranění, většinou se podaří smazat 80 - 90 % informací. V prvé řadě je nutné zjistit rozsah digitálních stop a kde se nacházejí. Poté již nastává nejtěžší fáze a to jejich odstranění.

Odstranění **aktivních** digitálních stop uživatele je nejjednodušší v případě, že uživatel sám tyto zdroje spravuje. Jedná se především o osobní blogy uživatelů, webové stránky, vlastní diskuze atp. Horší možnost odstranění přichází v případech sociálních sítí. Tam již uživatelé nemají plnou kontrolu nad sdílenými daty a zpravidla jsou vázáni přijmutím licenčních podmínek pro používaní těchto sítí. S tím však souvisejí povolení, která umožňují těmto sítím libovolné nakládání s našimi poskytnutými informacemi a obsahem těmto stranám.

Pokud se uživatel rozhodne pro zrušení jeho účtu na sociálních sítích, je třeba si uvědomit licenční podmínky jednotlivých sítí, které se liší především ve způsobu smazání dat. Tímto způsobem je smazání profilu „na oko“ uživatele, kdy sice dojde ke smazání profilu včetně nahraných souborů, ale informace o uživateli zůstavají stále uloženy na serverech. Tyto informace tedy nesou riziko zneužití, například, pokud dojde k útoku hackery.[61]

Zajímavou stránkou pro odhlašování se z jednotlivých služeb a sociálních sítí je stránka *http://justdelete.me/*, která obsahuje seznam nejznámějších webových služeb a sociálních sítí. Dále ukazuje složitost odstranění uživatelova účtu a informace, jakým způsobem lze účty smazat.

Odstranění **pasivních** digitálních stop je složitější než aktivních. Jedná se především o profily u zájmových reklamních společností, které monitorují uživatele a poté na ně aplikují cílené reklamy. Velkou roli při odstranění těchto stop hraje především doba uchovávání dat a odstranění na základě jednotlivých licenčních podmínek.

Jako příklad bych uvedl reklamní společnost Ogilvy & Mather, která je dle celosvětové statistiky na jedné z předních pozic [62]. Tato společnost v prohlášení udává, že sbírá a uchovává informace o uživatelích, kteří tyto informace dobrovolně poskytli. Tyto

[61] ROZMAJZL, Lukáš. *Jak smazat digitální stopu* [online].
[62] *Top 50 Ad Agencies* [online].

informace obsahují především uživatelovo jméno, e-mailovou adresu, bydliště atd. Zároveň však tato společnost automaticky sbírá data skrz cookies a je schopná rozpoznat např. uživatelův internetový prohlížeč, typ operačního systému, chování uživatele na internetu. V prohlášení je dále, že společnost může kontaktovat uživatele a nabízet mu služby na základě sdělených informací. Společnost dále nemůže zaručit, že informace uložené na jejích serverech a sítích nemohou být zneužity třetími stranami. Tato společnost neposkytuje žádné informace o době ukládání získaných informací a neumožňuje uživatelům manipulovat s již sdílenými daty. Tyto informace však lze částečně omezit za pomocí metod opt-out nebo cookies.[63]

Další možností odstranění pasivní stopy je formulář společnosti Google, pomocí něhož lze požádat o odstranění údajů o uživateli ve výsledcích vyhledávání. Tato možnost se však stahuje pouze na obyvatele Evropy. K žádosti je třeba doložit digitální kopii průkazu totožnosti uživatele. Dále je třeba uvést odkazy na adresy, které mají být smazány, a udán důvod smazání. Pak již zbývá žádost schálit společností a poté dojde ke smazání osoby ve výsledcích vyhledávání.[64]

9 Konkrétní nástroje pro ochranu soukromí

Existuje mnoho nástrojů, kterými lze chránit uživatelovo soukromí v prostředí internetu. Tyto nástroje se liší především jejich dostupností, funkcemi a typem (zda jde o samostatný software nebo pouze plugin). Dle funkcí jsou zvoleny jednotlivé skupiny těchto nástrojů, které se zabývají klíčovými prvky v ochraně pasivních stop. Hlavním kritériem při výběru nástrojů byla jejich volná dostupnost a počet stažení programů uživateli. U každé skupiny je tak vycházeno z konkrétních statistik stažení daných programů.

9.1 Nástroje k odstranění uložených souborů na PC

Mezi hlavní nástroje pro sledování aktivit uživatelů patří již několikrát v práci zmíněné soubory cookies, které se ukládají přes prohlížeč na pevný disk uživatele. Pokud uživatel nevyužívá nástroj pro blokování ukládání a přepisování cookies, je třeba tyto soubory pravidelně odstraňovat. Většina dnes používaných prohlížečů tuto funkci v základu

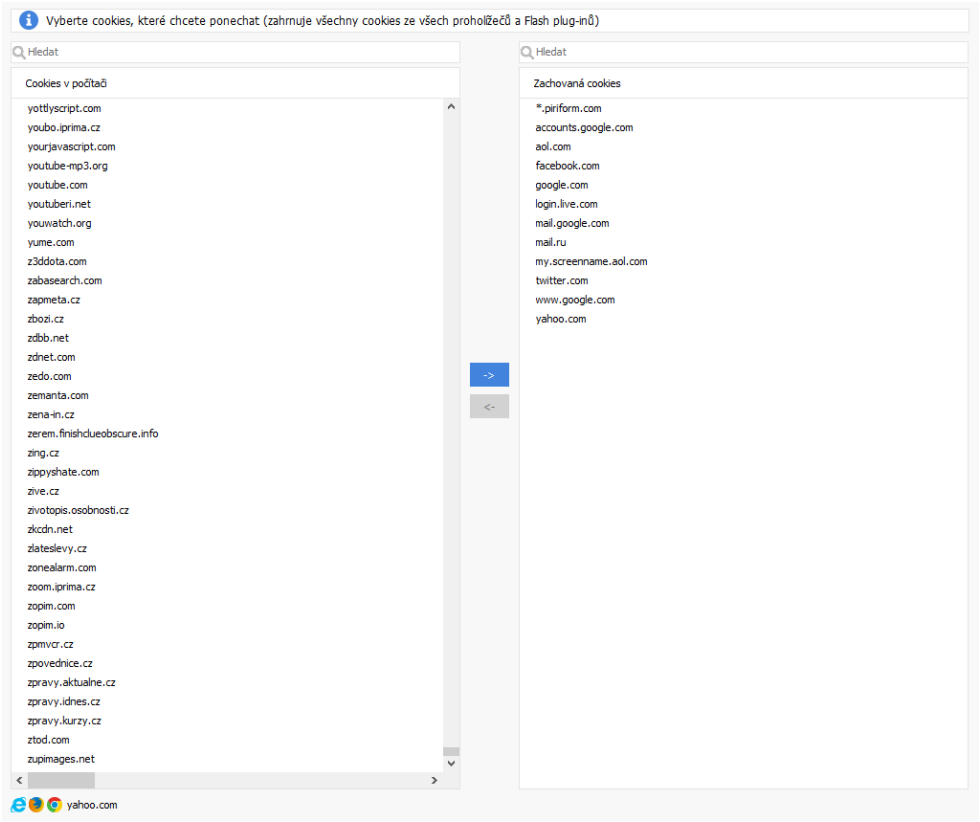
[63] *Ogilvy: Privacy Policy* [online].
[64] EUROZPRÁVY.CZ. *Google zavádí novou službu: Chcete zamést stopy? Nechte se smazat* [online].

umožňují, avšak neumožňují mazání cookies typu flash a Silverlight. Proto je třeba použít dodatečné softwarové nástroje, které toto mazání umožňují.

Pro porovnání byly vybrány nejvíce stahované, zdarma dostupné programy dle webové stránky www.download.cnet.com [65]. Kritériem pro toto porovnání byl počet funkcí a s tím i související počet druhů souborů, které umí tyto programy odstranit.

9.1.1 CCleaner

CCleaner od společnosti Piriform je jeden z nejstahovanějších a nejpopulárnějších volně dostupných nástrojů. Program slouží především pro optimalizaci systému a pro odstraňování nepotřebných souborů a registrů. Zároveň však umožňuje odstranit soubory spojené s prohlížeči (podpora téměř všech prohlížečů) jako např. internetovou cache, historii procházení a stahování, uložená hesla a formuláře a především cookies (i flash). Uživatel má dále možnost si vytvořit seznam cookies, na které se mazání nebude vztahovat (viz Obrázek 5). Toho lze využít především u užitečných cookies, které slouží k zapamatování nastavení na navštívených webových stránkách.



Obrázek 6 - Správa cookies v CCleaner (zdroj: vlastní archiv autora)

[65] *Download.cnet: Maintenance & Optimization for Windows* [online].

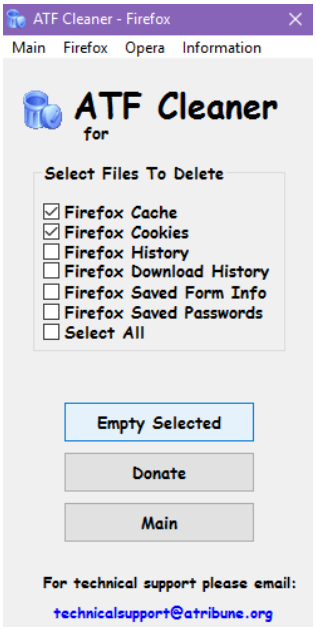
9.1.2 Flash Cookie Cleaner

Flash cookie cleaner je program, který se zaměřuje především a pouze na vyhledání a odstranění flash cookies. Oproti CCleaneru umí zobrazit i datum vytvoření jednotlivých cookies a nabízí i možnost pravidelného skenu a odstranění flash cookies (denně, týdně, měsíčně). Nástroj též vytvářet výjimky v cookies, aby nedošlo k smazání „chtěných“ cookies. Nástroj je přehledný a plně slouží k jeho primárnímu účelu.

Obrázek 7 - Nástroj Flash Cookie Cleaner (zdroj: vlastní archiv autora)

9.1.3 ATF Cleaner

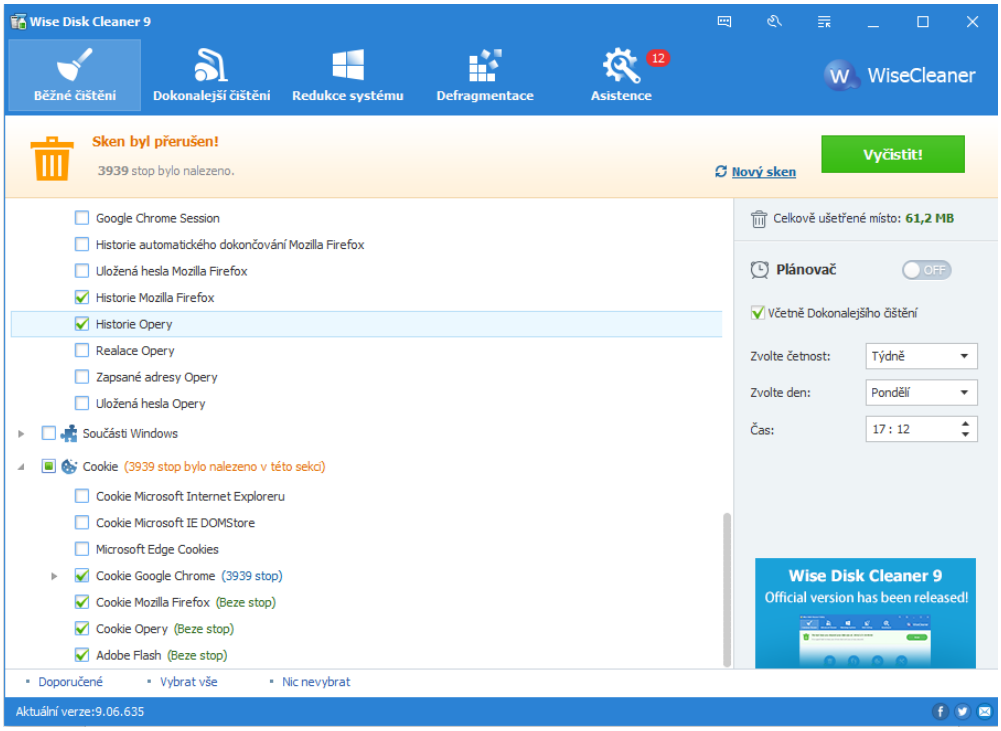
Tento nástroj nevyžaduje instalaci a po stažení je přímo spustitelný. Jedná se o velmi jednoduchý nástroj, který se zaměřuje na odstranění souborů prohlížečů a částečně i na správu systémových souborů. Podporuje mazání cache, cookies, historie stahování a procházení, uložených formulářů a hesel. Nepodporuje však mazání flash cookies. Další nevýhodou je mazání pouze v rámci IE, Mozilly Firefox a Opery. Dále programu chybí tvoření cookies výjimek. Program tedy maže vždy celé vybrané položky.



Obrázek 8 - ATF Cleaner (zdroj: vlastní archiv autora)

9.1.4 Wise Disk Cleaner

Wise Disk Cleaner je dalším nástrojem pro optimalizaci operačního systému. Obsahuje mimo jiné i funkce pro odstranění internetových souborů jako jsou cookies, flash cookies, uložená hesla a historii, formuláře a webové cache. Je velmi podobný CCleaneru a umožňuje i vybraná cookies přidávat do výjimek. Lze také nastavit plánovač spouštění skenování a čištění souborů.



Obrázek 9 - Wise Disk Cleaner (zdroj: vlastní archiv autora)

9.1.5 Konečné porovnání a zhodnocení

Na základě funkcí jednotlivých nástrojů byla sestavena výsledná tabulka s přehledem parametrů, jejichž odstranění zajišťují či nezajišťují vybrané nástroje. Celkové hodnocení pak bylo sestaveno jako součet bodů na základě bodování podle klíče: 1 bod - splňuje zcela (v tabulce Ano), 0 bodů – nesplňuje (v tabulce Ne). Nejlépe hodnocen je ten nástroj, který se nejvíce blíží maximu možných bodů (100 % odpovídá maximu možných bodů).

	CCleaner	Flash Cookie Cleaner	ATF Cleaner	Wise Disk Cleaner
Cookies	Ano	Ne	Ano	Ano
Flash cookies	Ano	Ano	Ne	Ano
Historie prohlížení a stahování	Ano	Ne	Ano	Ano
Uložená hesla a formuláře	Ano	Ne	Ano	Ano
Internetová cache	Ano	Ne	Ano	Ano
Podpora mnoha prohlížečů	Ano	Ne	Ne	Ano
GUI	Velmi přehledné	Velmi přehledné	Velmi přehledné	Méně přehledné
Součet bodů	7 ze 7 (100%)	2 ze 7 (29%)	5 ze 7 (71%)	6 ze 7 (86%)

Tabulka 1 - Porovnání nástrojů pro odstranění uložených souborů na PC (zdroj: vlastní archiv autora)

Z výsledného porovnání vyšel nejlépe CCleaner, který je velmi komplexním nástrojem s mnoha funkcemi. Jak pro optimalizaci systému a nepotřebných souborů, tak pro odstranění sledovacích souborů (cookies a historie). Především díky jeho jednoduchosti, přehlednému grafickému rozhraní, kompatibilitě a dostupnosti je jedním z nejstahovanějších a nejpoužívanějších softwarů v této kategorii. Druhým v pořadí skončil nástroj Wise Disk Cleaner, který má mnoho společných funkcí s CCleanerem. Obsahuje však o něco menší počet funkcí (především co se optimalizace týče) a je méně přehledný. Na třetím místě se umístil ATF Cleaner, který bohužel neumožňuje odstranění flash cookies souborů a umí vyčistit pouze soubory z pár webových prohlížečů. Nabízí tak

víceméně funkce, které nabízejí i webové prohlížeče v jejich nastavení. Poslední program s názvem Flash Cookie Cleaner dopadl sice v hodnocení nejhůře, protože se zaměřuje pouze na mazání flash cookies, ale v tomto ohledu předčil ATF Cleaner, který toto řešení nenabízí. Flash Cookie Cleaner také umožňuje vytvářet výjimky flash cookies a je velmi přehledný a intuitivní.

9.2 Nástroje, které zajišťují anonymitu na internetu

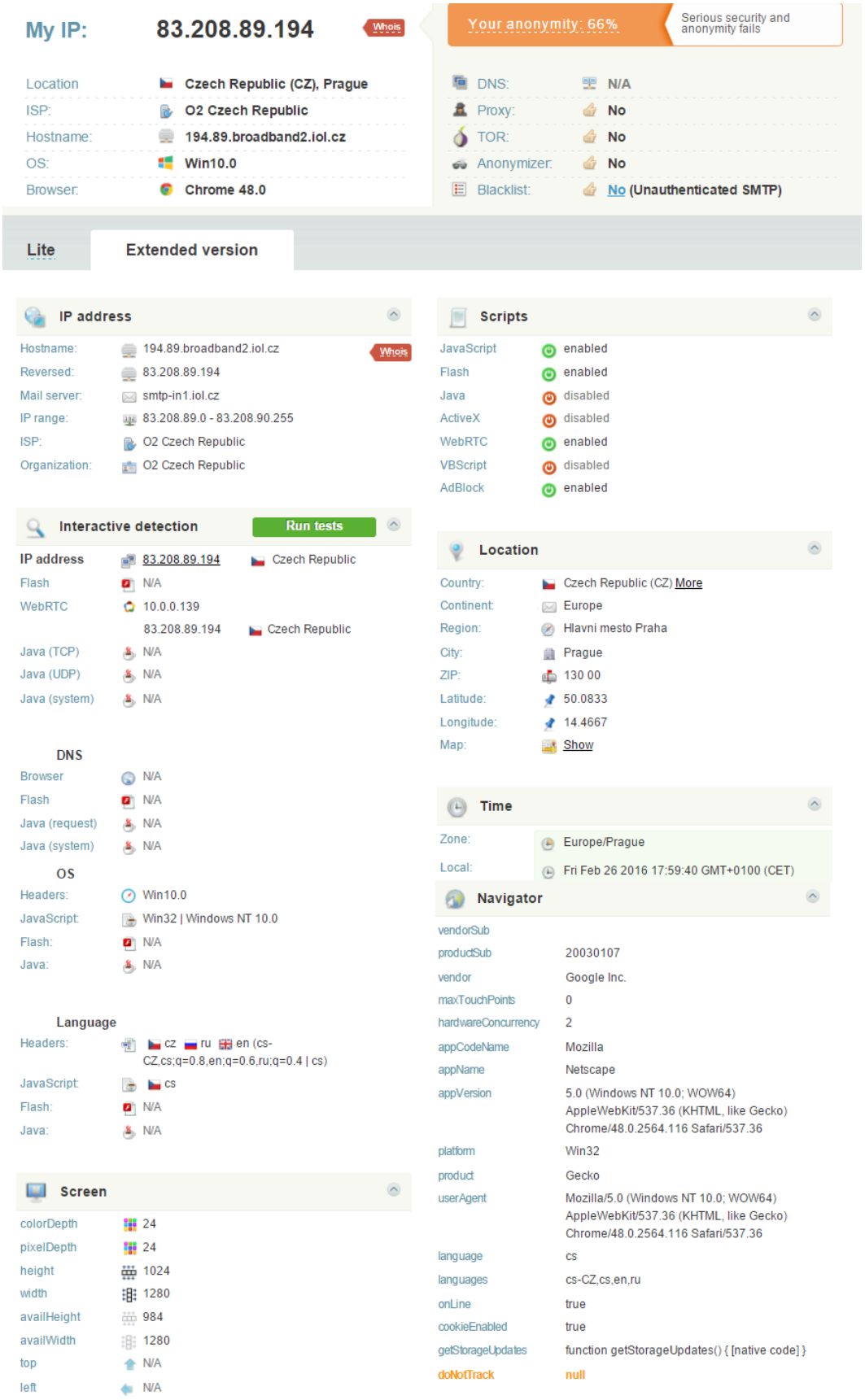
Dalšími nástroji, kterými lze chránit soukromí uživatelů, jsou anonymizační nástroje. O těchto nástrojích již byla řeč v kapitole 8.2.2. Pro komparaci byly použity volně dostupné a nejvíce stahované nástroje Tor [66] a I2P [67] z portálu www.download.cnet.com.[68] Pro další porovnání byl použit i již zmíněný webový proxy server WebProxy.

Cílem komparace je porovnat tyto nástroje a zjistit, kolik anonymity poskytují uživatelům a kolik informací o uživatlích lze i přes jejich použití získat. Anonymní režimy jednotlivých prohlížečů nejsou zahrnuty do výsledného porovnání, protože nenabízí téměř žádnou anonymitu - pouze neukládají historii procházení a stahování. V rámci komparace byly použity online testy anonymity Whoer [69] a IP Check. [70]

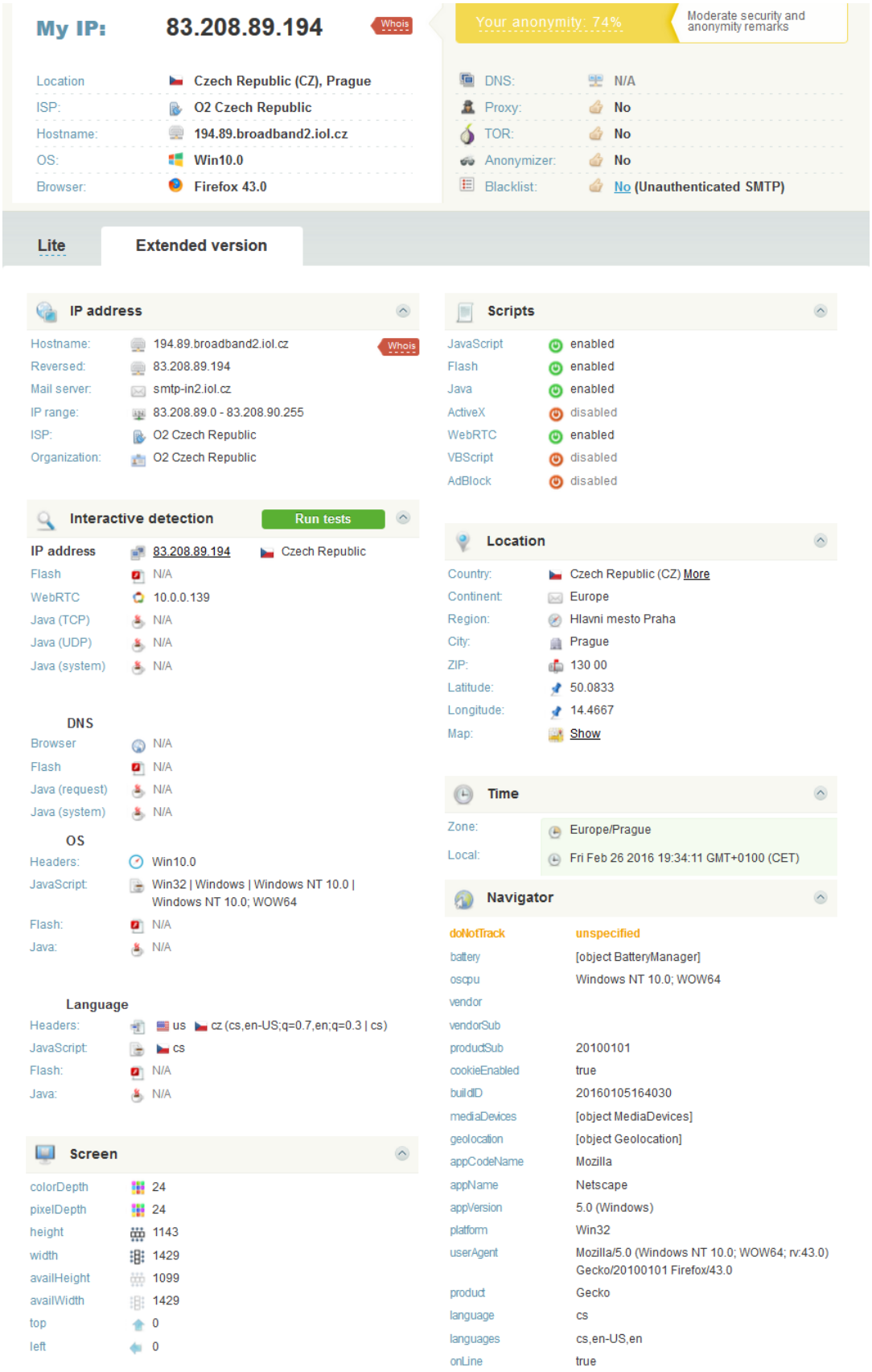
9.2.1 Běžné internetové prohlížeče

Pro porovnání možností ochrany, které nabízejí nástroje Tor, I2P a WebProxy, je třeba zjistit, kolik informací lze o uživateli zjistit během používání klasického internetového prohlížeče. Pro tyto účely byly vybrány tři velmi známé prohlížeče a bylo provedeno pro přehlednost jejich testování přes Whoer.net.

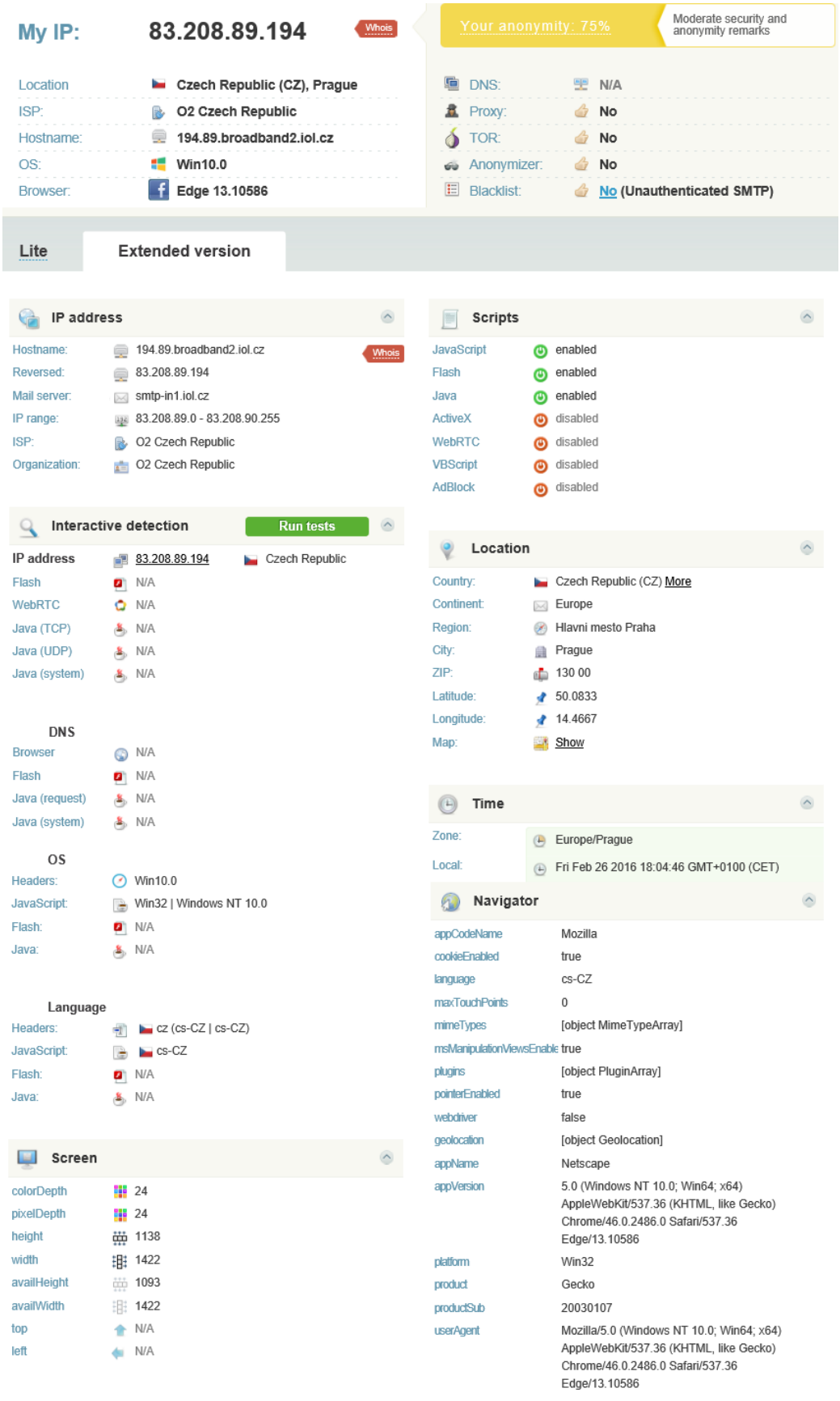
[66] *Tor Browser for Windows* [online].
[67] *I2P: Clean installs* [online].
[68] *Download.cnet: Web Browsers for Windows* [online].
[69] *Whoer* [online].
[70] *IP check* [online].



Obrázek 10 - Test anonymity prohlížeče Google Chrome v.48.0 (zdroj: vlastní archiv autora)



Obrázek 11- Test anonymity prohlížeče Mozilla Firefox v.43.0 (zdroj: vlastní archiv autora)



Obrázek 12 - Test anonymity prohlížeče Microsoft Edge v.13.10586 (zdroj: vlastní archiv autora)

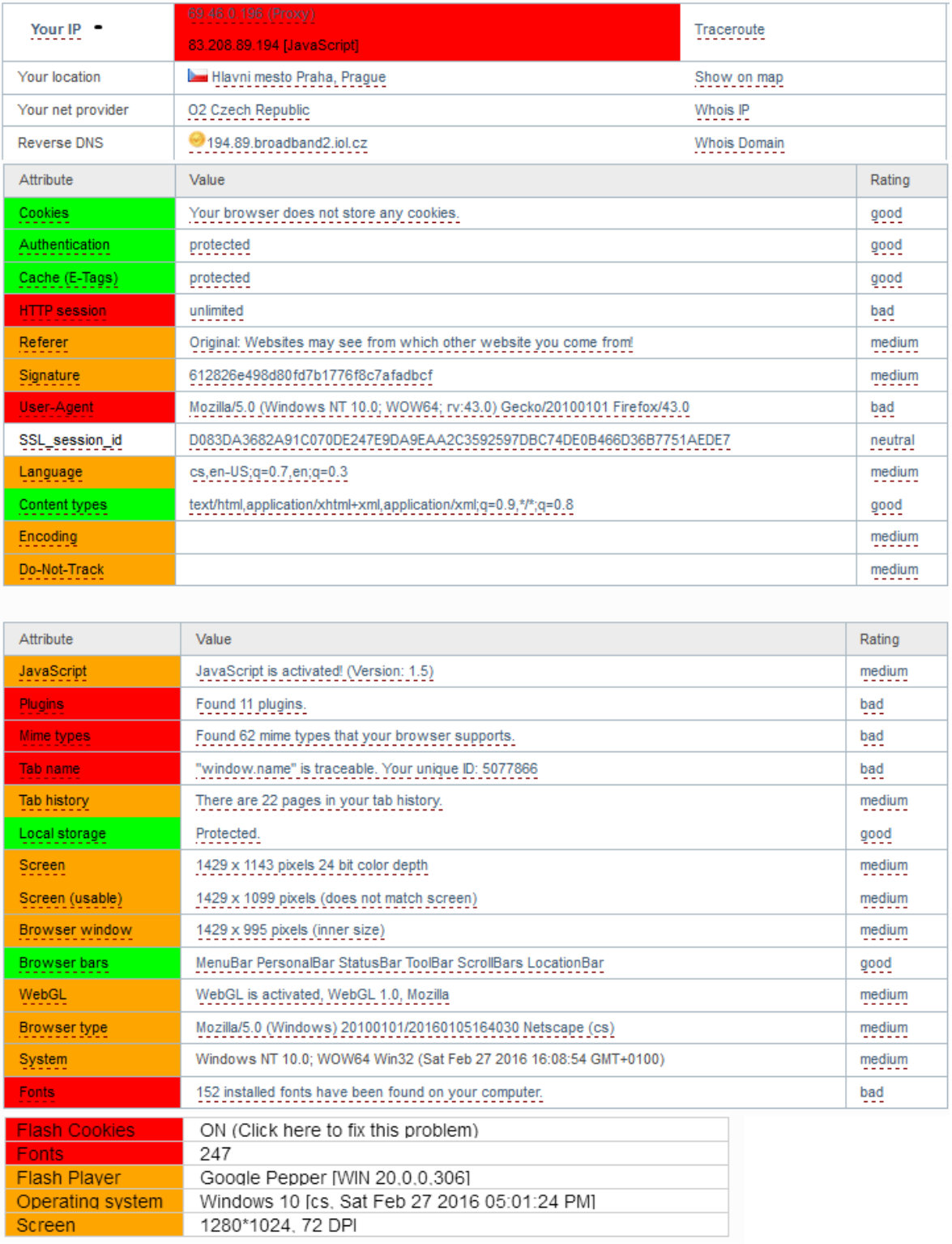
Z těchto testů vyplývá, že při běžném surfování klasickými prohlížeči lze o uživateli zjistit poměrně dost informací. Všechny tyto běžné prohlížeče nabízejí v základu velmi malou ochranu uživatelova soukromí. Spousta aktivit je přes tyto prohlížeče poměrně snadno zjistitelná a sledovatelná. Jak vidno z výsledných testů, každá navštívená stránka zjistí informace jako uživatelovu IP adresu, jeho používaný OS, poskytovatele připojení (ISP), přibližnou polohu a místní čas, verzi prohlížeče a mnoho dalších. Další problém představují povolené flash cookies u všech testovaných prohlížečů. Dále pak v kolonce „Navigator“ jsou u všech prohlížečů povoleny soubory cookies a viditelné informace o User agentu, který poskytuje webovým stránkám informace o uživatelově OS a s flash a java aplikacemi tvoří otisk prohlížeče.

Výsledky testů jednotlivých prohlížečů jsou prakticky stejné a poslouží především jako výchozí bod pro další porovnání nástrojů.

9.2.2 Webproxy.com

O webovém anonymizéru WebProxy již bylo řečeno v kapitole 8.2.2 Anonymní módy. V následující části bude tento anonymizér otestován přes online test IP Check, který umožňuje oproti Whoeru zobrazit i hodnocení bezpečnosti atributů.

Při provádění testování byly v nastavení WebProxy zvoleny parametry: Nepovolovat cookies.



Your IP	69.46.0.196 (Proxy) 83.208.89.194 [JavaScript]	Traceroute
Your location	Hlavní město Praha, Prague	Show on map
Your net provider	O2 Czech Republic	Whois IP
Reverse DNS	194.89.broadband2.iol.cz	Whois Domain

Attribute	Value	Rating
Cookies	Your browser does not store any cookies.	good
Authentication	protected	good
Cache (E-Tags)	protected	good
HTTP session	unlimited	bad
Referer	Original: Websites may see from which other website you come from!	medium
Signature	612826e498d80fd7b1776f8c7afadbcf	medium
User-Agent	Mozilla/5.0 (Windows NT 10.0; WOW64; rv:43.0) Gecko/20100101 Firefox/43.0	bad
SSL_session_id	D083DA3682A91C070DE247E9DA9EAA2C3592597DBC74DE0B466D36B7751AEDE7	neutral
Language	cs,en-US;q=0.7,en;q=0.3	medium
Content types	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8	good
Encoding		medium
Do-Not-Track		medium

Attribute	Value	Rating
JavaScript	JavaScript is activated! (Version: 1.5)	medium
Plugins	Found 11 plugins.	bad
Mime types	Found 62 mime types that your browser supports.	bad
Tab name	"window.name" is traceable. Your unique ID: 5077866	bad
Tab history	There are 22 pages in your tab history.	medium
Local storage	Protected.	good
Screen	1429 x 1143 pixels 24 bit color depth	medium
Screen (usable)	1429 x 1099 pixels (does not match screen)	medium
Browser window	1429 x 995 pixels (inner size)	medium
Browser bars	MenuBar PersonalBar StatusBar ToolBar ScrollBars LocationBar	good
WebGL	WebGL is activated, WebGL 1.0, Mozilla	medium
Browser type	Mozilla/5.0 (Windows) 20100101/20160105164030 Netscape (cs)	medium
System	Windows NT 10.0; WOW64 Win32 (Sat Feb 27 2016 16:08:54 GMT+0100)	medium
Fonts	152 installed fonts have been found on your computer.	bad

Flash Cookies	ON (Click here to fix this problem)
Fonts	247
Flash Player	Google Pepper [WIN 20,0,0,306]
Operating system	Windows 10 [cs, Sat Feb 27 2016 05:01:24 PM]
Screen	1280*1024, 72 DPI

Obrázek 13 - Test anonymity přes Webproxy.com (zdroj: vlastní archiv autora)

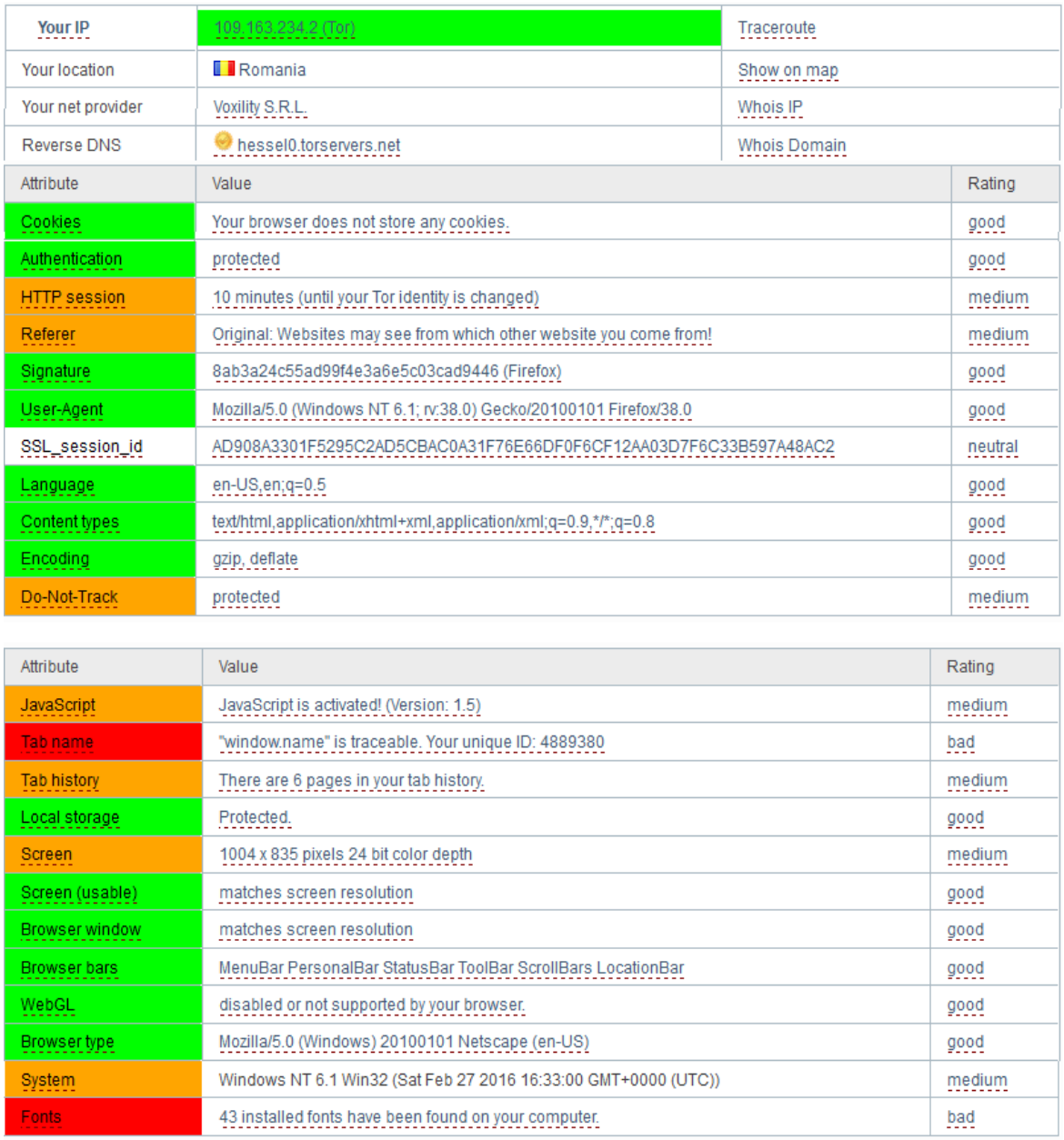
Hlavním úkolem webových proxy serverů je skrytí uživatelovy vlastní IP adresy, to se bohužel při testu nepodařilo. Zpočátku se sice načetla IP adresa proxy serveru, ale po chvíli dojde k její záměně za uživatelovu skutečnou. Je bohužel dáno speciálním Java scriptem,

který odhalí adresu, odkud byl dotaz poslán. Tento script však nemusí obsahovat každá webová stránka. Dojde tedy k rozpoznání naší pravé IP adresy, polohy a poskytovatele internetových služeb. Soubory cookies však oproti běžným prohlížečům nejsou ukládány na uživatelův disk, ověřování (Authentication) a Cache (E-Tags) jsou chráněny, tzn. třetí strany nemohou sledovat uživatelovy aktivity. HTTP session však není chráněno a dovoluje poskytovateli internetových služeb spojovat uživatelovy požadavky a na základě nich pak získat přehled o jeho zájmech. User agent je viditelný a zanechává tak otisk prohlížeče. Flash cookies jsou povoleny.

V závěru lze říci, že webové proxy nabízejí pouze nepatrná vylepšení oproti klasickým webovým prohlížečům. To nejdůležitější - naše IP adresa však pomocí nich stále není stoprocentně chráněna.

9.2.3 Tor

Následující test anonymity byl proveden přes nainstalovaný Tor Browser, stažený z oficiálních stránek. Jako nástroj pro online testování anonymity byl opět použit IP Check.



Your IP	109.163.234.2 (Tor)	Traceroute
Your location	Romania	Show on map
Your net provider	Voxility S.R.L.	Whois IP
Reverse DNS	hessel0.torservers.net	Whois Domain

Attribute	Value	Rating
Cookies	Your browser does not store any cookies.	good
Authentication	protected	good
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:38.0) Gecko/20100101 Firefox/38.0	good
SSL_session_id	AD908A3301F5295C2AD5CBAC0A31F76E66DF0F6CF12AA03D7F6C33B597A48AC2	neutral
Language	en-US,en;q=0.5	good
Content types	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8	good
Encoding	gzip, deflate	good
Do-Not-Track	protected	medium

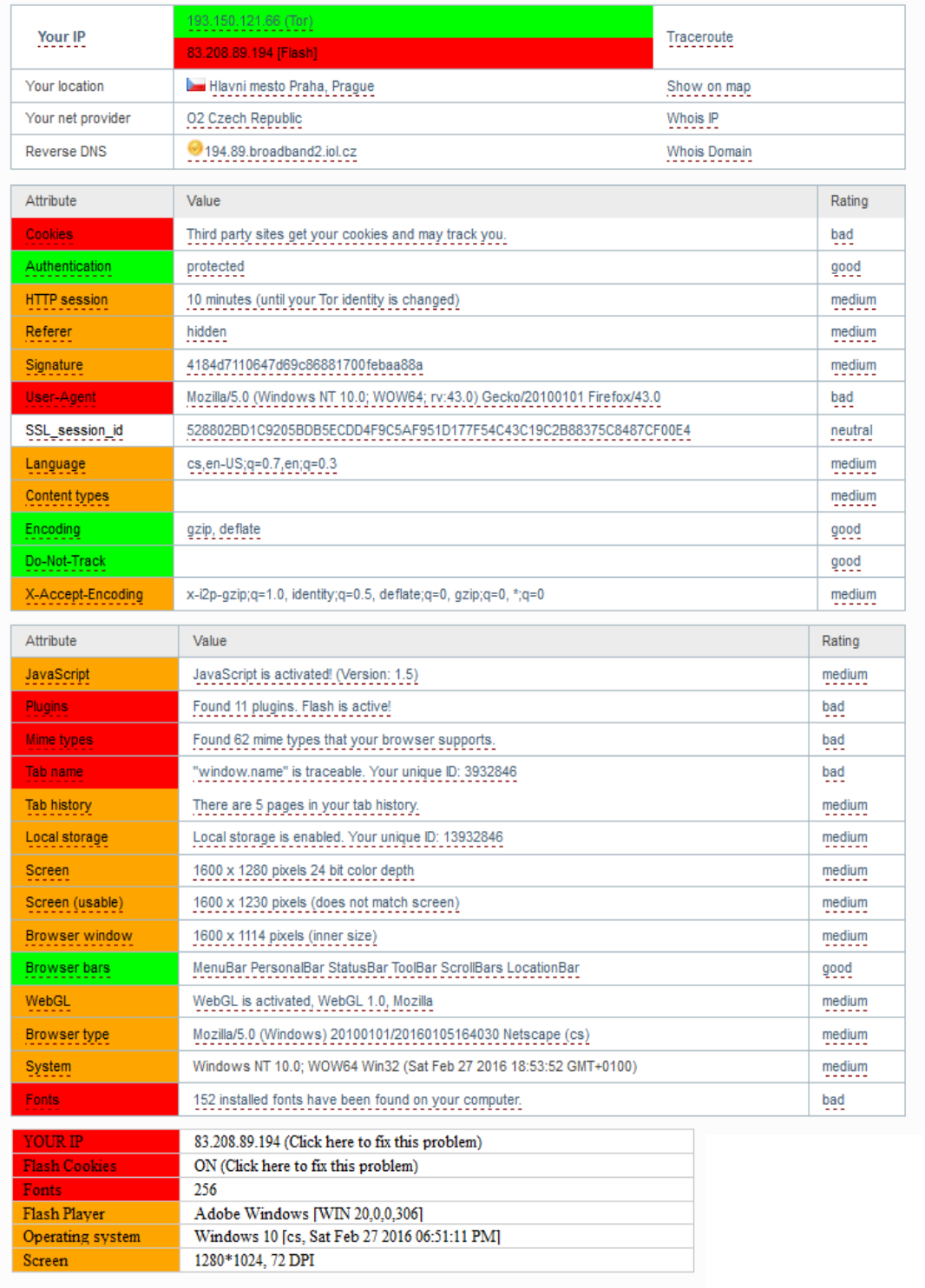
Attribute	Value	Rating
JavaScript	JavaScript is activated! (Version: 1.5)	medium
Tab name	"window.name" is traceable. Your unique ID: 4889380	bad
Tab history	There are 6 pages in your tab history.	medium
Local storage	Protected.	good
Screen	1004 x 835 pixels 24 bit color depth	medium
Screen (usable)	matches screen resolution	good
Browser window	matches screen resolution	good
Browser bars	MenuBar PersonalBar StatusBar ToolBar ScrollBars LocationBar	good
WebGL	disabled or not supported by your browser.	good
Browser type	Mozilla/5.0 (Windows) 20100101 Netscape (en-US)	good
System	Windows NT 6.1 Win32 (Sat Feb 27 2016 16:33:00 GMT+0000 (UTC))	medium
Fonts	43 installed fonts have been found on your computer.	bad

Obrázek 14 - Test anonymity sítě Tor (zdroj: vlastní archiv autora)

U testu sítě Tor jsme již dostali o poznání lepších výsledků než u webové proxy. Skutečná IP adresa uživatele je již skrytá a s ní je i jiná poloha a poskytovatel připojení. Cookies soubory nejsou ukládány na lokální úložiště, autentifikace je chráněná. HTTP session však zasílají informace o předchozí uživatelově navštívené stránce. HTTP session se však mění každých 10 minut automaticky a tím lze zabránit sledování poskytovatelem. Jelikož Tor zabraňuje načítání Flash a Java scriptů pomocí funkce NoScript, chybí ve výsledcích testu a tedy flash cookies nejsou přijímány. Identifikace uživatele využívajícího síť Tor je prakticky nemožná, protože všichni uživatelé mají stejný prohlížeč, podpis a jazyk.

9.2.4 I2P

Ke správnému fungování I2P je třeba nainstalovat klienta a nastavit proxy server. Jako proxy server byl stažen a nakonfigurován plugin FoxyProxy pro Mozillu Firefox. Jako nástroj pro online testování anonymity byl opět použit IP Check.



Your IP	193.150.121.66 (Tor) 83.208.89.194 [Flash]	Traceroute
Your location	Hlavní město Praha, Prague	Show on map
Your net provider	O2 Czech Republic	Whois IP
Reverse DNS	194.89.broadband2.iol.cz	Whois Domain

Attribute	Value	Rating
Cookies	Third party sites get your cookies and may track you.	bad
Authentication	protected	good
HTTP session	10 minutes (until your Tor identity is changed)	medium
Referer	hidden	medium
Signature	4184d7110647d69c86881700febaa88a	medium
User-Agent	Mozilla/5.0 (Windows NT 10.0; WOW64; rv:43.0) Gecko/20100101 Firefox/43.0	bad
SSL_session_id	528802BD1C9205BDB5ECDD4F9C5AF951D177F54C43C19C2B88375C8487CF00E4	neutral
Language	cs,en-US;q=0.7,en;q=0.3	medium
Content types		medium
Encoding	gzip, deflate	good
Do-Not-Track		good
X-Accept-Encoding	x-i2p-gzip;q=1.0, identity;q=0.5, deflate;q=0, gzip;q=0, *;q=0	medium

Attribute	Value	Rating
JavaScript	JavaScript is activated! (Version: 1.5)	medium
Plugins	Found 11 plugins. Flash is active!	bad
Mime types	Found 62 mime types that your browser supports.	bad
Tab name	"window.name" is traceable. Your unique ID: 3932846	bad
Tab history	There are 5 pages in your tab history.	medium
Local storage	Local storage is enabled. Your unique ID: 13932846	medium
Screen	1600 x 1280 pixels 24 bit color depth	medium
Screen (usable)	1600 x 1230 pixels (does not match screen)	medium
Browser window	1600 x 1114 pixels (inner size)	medium
Browser bars	MenuBar PersonalBar StatusBar ToolBar ScrollBars LocationBar	good
WebGL	WebGL is activated, WebGL 1.0, Mozilla	medium
Browser type	Mozilla/5.0 (Windows) 20100101/20160105164030 Netscape (cs)	medium
System	Windows NT 10.0; WOW64 Win32 (Sat Feb 27 2016 18:53:52 GMT+0100)	medium
Fonts	152 installed fonts have been found on your computer.	bad

YOUR IP	83.208.89.194 (Click here to fix this problem)
Flash Cookies	ON (Click here to fix this problem)
Fonts	256
Flash Player	Adobe Windows [WIN 20,0,0,306]
Operating system	Windows 10 [cs, Sat Feb 27 2016 06:51:11 PM]
Screen	1280*1024, 72 DPI

Obrázek 15 - Test anonymity sítě I2P (zdroj: vlastní archiv autora)

Z výsledků testu I2P vyplývá, že IP adresa uživatele je zpočátku podobně jako u webové proxy jiná než IP uživatele. Po pár sekundách se ale opět změní na uživatelovu díky flash scriptu obsaženém na stránce. Je tak tedy odhalena uživatelova pravá IP adresa, poloha a poskytovatel připojení. Další nastavení je už závislé na tunelu uživatele, na který jsme napojeni. Cookies jsou tedy bohužel povoleny, avšak ověřování je aktivní a chráněné. HTTP session je podobně jako u Toru měněno každých 10 minut automaticky. Referer je skrytý a tedy neposkytuje informace o předchozí navštívené stránce. Local storage je povolené, tzn., že mohou být ukládány identifikační soubory a pluginy do počítače. Flash cookies jsou aktivní.

Práce s I2P byla velmi pomalá vzhledem k nízkému počtu routerů (klientů) a test se načítal v řádu minut a načetl se až na několikátý pokus.

9.2.5 Konečné porovnání a zhodnocení

V závislosti na funkcích vybraných anonymizačních nástrojů byla sestavena výsledná porovnávací tabulka s parametry, které umožňují chránit naši identitu při pohybu na internetu. Jak již bylo řečeno, klasické prohlížeče jsou zahrnuty do tabulky pro znázornění, jaké informace lze zjistit o uživateli při pohybu internetem. Celkové hodnocení pak bylo sestaveno jako součet bodů na základě bodování podle klíče: 1 bod - splňuje zcela (v tabulce Ano), 0,5 bodů – splňuje částečně (v tabulce Ano/Ne) a 0 bodů – nesplňuje (v tabulce Ne). Nejlépe hodnocen je ten nástroj, který se nejvíce blíží maximu možných bodů (100 % odpovídá maximu možných bodů). Hodnota Ano/Ne je závislá na individuálním nastavení (klasické prohlížeče mohou přijímat nebo blokovat cookies) či přítomnosti skriptu, který ovlivní výsledný výsledek testu nástroje (Webproxy).

	Klasické prohlížeče	Webproxy.com	Tor	I2P
IP adresa	Ne	Ano/Ne	Ano	Ano/Ne
Poloha uživatele	Ne	Ano/Ne	Ano	Ano/Ne
ISP	Ne	Ano/Ne	Ano	Ano/Ne
Cookies	Ano/Ne	Ano	Ano	Ne
Flash cookies	Ne	Ne	Ano	Ne
Authentication	Ne	Ano	Ano	Ano
HTTP session	Ne	Ne	Ano	Ano
Referer	Ne	Ne	Ne	Ano
Local Storage	Ne	Ano	Ano	Ne
Otisk prohlížeče (User Agent)	Ne	Ne	Ano	Ne
Součet bodů	0,5 z 10 (5%)	4,5 z 10 (45%)	9 z 10 (90%)	4,5 z 10 (45%)

Tabulka 2 - Porovnání anonymizačních nástrojů (zdroj: vlastní archiv autora)

Z výsledků komparace je zřejmé, že největší ochranu soukromí umožňuje síť Tor, která obstála téměř ve všech parametrech, pouze Referer, který podává informace o předchozí návštěvě stránky, dopadl lépe u sítě I2P. Webový anonymizér WebProxy skončil na stejném hodnocení spolu s I2P. Hodnocení I2P je závislé na P2P komunikaci a nastavení je tedy závislé na klientovi, ke kterému se uživatel napojuje a jaké nastavení ochrany soukromí tento klient má. Na druhou stranu je I2P síť velmi pomalá. Nejlepším anonymizačním nástrojem v ochraně soukromí uživatele je tedy prohlížeč Tor.

9.3 Nástroje, které zabraňují sledování aktivit uživatele

V následující části bude řeč především o nástrojích, které umožňují zamezit monitorování aktivit uživatelů při jejich pohybu na internetu. Nejběžnějším a nejjednodušším způsobem z pohledu uživatele je instalace pluginů k běžným prohlížečům. Tyto nástroje nevyžadují po uživatelích téměř žádnou další konfiguraci a uživatelovy znalosti. Tím se liší především

od již výše zmíněných samostaných softwarových nástrojů. Právě díky své jednoduchosti a flexibilitě jsou hojně využívány širokým spektrem uživatelů.

Pro porovnání byly použity dle statistik nejvíce stahované pluginy[71] zabývající se touto problematikou. Všechny pluginy byly nainstalovány a otestovány v prohlížeči Google Chrome, jakožto nejvyužívanějšímu prohlížeči na světě. [72] Testování probíhalo přes webovou aplikaci Panopticlick[73], která se zabývá testováním bezpečnosti prohlížečů před sledováním. Každý plugin byl testován samostatně a odděleně, aby nedošlo k jejich vzájemnému ovlivňování a nekompatibilitě.

Pro další porovnání jednotlivých pluginů je vhodné, nejdříve provést test anonymity pro prohlížeč bez aktivních pluginů.

Test	Result
Is your browser blocking tracking ads?	✗ no
Is your browser blocking invisible trackers?	✗ no
Does your browser unblock 3rd parties that promise to honor Do Not Track?	✗ no
Does your browser protect from fingerprinting?	✗ your browser has a unique fingerprint

Obrázek 16 - Výsledky testu sledování aktivit bez použití jakéhokoliv pluginu (zdroj: vlastní archiv autora)

Z výsledku testu sledování při použití AdBlock Plus je zřejmé, že je aktivní blokování reklam a neviditelných sledovacích zařízení. Dále je patrné, že AdBlock Plus neodblokovává třetí strany, které slibují, že ctí prohlášení Do Not Track[74] (uživatel může informovat webovou stránku, že si nepřeje být sledován prostřednictvím HTTP hlavičky). Po použití AdBlock Plus je však stále zanecháván otisk prohlížeče, který umožňuje mimo jiné i ignorovat Do Not Track požadavek uživatelů.

[71] *Internetový obchod Chrome* [online].
[72] *W3Schools: Browser Statistics* [online].
[73] *Panopticlick: Is your browser safe against tracking?* [online].
[74] *EFF: A privacy-friendly Do Not Track (DNT) Policy* [online].

9.3.1 Ghostery

Plugin Ghostery je k dispozici pro všechny nejpoužívanější webové prohlížeče. [75] Ghostery má vlastní knihovnu trackerů, která je pravidelně aktualizována. Princip Ghostery spočívá na detekci neviditelných sledacích zařízení na uživatelově právě navštívené stránce. Nalezená trackovací zařízení nejsou primárně zablokována, o jejich případné blokaci rozhoduje až uživatel. Ghostery dále poskytuje velmi detailní přehled o těch zařízeních. Trackery jsou dále přehledně rozděleny do jednotlivých kategorií což usnadňuje jejich celkové filtrování.

Ghostery umí najít a zablokovat například soubory cookies vybraných společností, pixelové tagy,[76] vložené pluginy (sociálních sítí atp.), objekty vložené přes JavaScript, Iframy (v kterých může být vnořena jiná webová stránka) a v poslední řadě zabraňuje nechtěnému přesměrování na jinou webovou stránku.

S touto blokací může ovšem souviset nefunkčnost některých funkcí na webových stránkách. Proto Ghostery umožňuje nastavit konkrétní výjimky a povolit tak daný prvek.

Test	Result
Is your browser blocking tracking ads?	✓ yes
Is your browser blocking invisible trackers?	✓ yes
Does your browser unblock 3rd parties that promise to honor Do Not Track?	✗ no
Does your browser protect from fingerprinting?	✗ your browser has a unique fingerprint

Obrázek 17 - Výsledky testu sledování aktivit s aktivním pluginem Ghostery (zdroj: vlastní archiv autora)

Výsledek testu vyšel úplně stejný jako při použití pluginu AdBlock Plus.

9.3.2 AdBlock Plus

AdBlock Plus je dalším velmi populárním pluginem, který především založen na blokování reklam, ale umožňuje i zabránit sledování online aktivit uživatelů. Jeho princip je založen

[75] *Ghostery: Download browser extension* [online].
[76] Malé obrazové soubory, které jsou umístěny ve zdrojovém kódu webové stránky

na seznamech filtrů, které obsahují pravidla, co přesně se má blokovat. Tyto seznamy jsou pravidelně aktualizovány a stahovány. Filtry lze přidávat i ručně, musí však odpovídat syntaxi. Také lze přidávat vlastní domény, pro které bude AdBlock Plus zakázán.

Adblock Plus umí blokovat nepříjemné reklamy, blikací bannery, facebookové reklamy, vyskakovací okna apod. Pro zabránění sledování (trackování) uživatelů je třeba přidat seznam filtrů Easy Privacy do uživatelova seznamu. Dále je zde možnost blokovat tlačítka sociálních sítí, které se nacházejí na mnoha webových stránkách. Tyto tlačítka shromažďují informace o uživatelích i když na ně vůbec nemusí kliknout. AdBlock Plus toto řeší opět použitím seznamu filtrů s názvem Antisocial. Nejpopulárnějším seznamem filtrů je EasyList, který umožňuje i odstranění Iframů, obrázků a objektů z webových stránek. AdBlock Plus tak nabízí poměrně komplexní řešení v ochraně soukromí uživatelů a to především za pomocí těchto seznamů spravovaných komunitou.[77]

Test	Result
Is your browser blocking tracking ads?	✓ yes
Is your browser blocking invisible trackers?	✓ yes
Does your browser unblock 3rd parties that promise to honor Do Not Track?	✗ no
Does your browser protect from fingerprinting?	✗ your browser has a unique fingerprint

Obrázek 18 - Výsledky testu sledování aktivit s aktivním pluginem AdBlock Plus (zdroj: vlastní archiv autora)

9.3.3 Privacy Badger

Plugin Privacy Badger je velmi jednoduchým anti-trackovacím programem. Není tak přímo zaměřen na blokování reklamy jako AdBlock Plus, ale soustředí se na zabránění sledování aktivit uživatele třetími stranami. Zaměřuje se především na ty strany, které nerespektují žádost Do Not Track, a tyto domény blokuje. Plugin si vede seznam domén třetích stran ukládajících na webové stránky obrázky, reklamy a skripty. Pokud vyhodnotí, že uživatele tyto strany sledují bez povolení, Privacy Badger zakáže tracker. Nedochází tak k omezení funkčnosti stránek, jelikož plugin pouze zakáže trackovací cookie třetí strany.

[77] *Easylist* [online].

Tato reakce na trackery je prováděna automaticky, ale lze ji nastavit ručně a to ve třech stupních: Zcela povolit, zcela zakázat a blokovat cookie.

Test	Result
Is your browser blocking tracking ads?	✓ yes
Is your browser blocking invisible trackers?	✓ yes
Does your browser unblock 3rd parties that promise to honor Do Not Track?	✓ yes
Does your browser protect from fingerprinting?	✗ your browser has a unique fingerprint

Obrázek 19 - Výsledky testu sledování aktivit s aktivním pluginem Privacy Badger (zdroj: vlastní archiv autora)

Oproti předchozím testům AdBlock Plus a Ghostery umožňuje Privacy Badger odblokovávat strany, které slibují, že budou dodržovat pravidla pro HTTP hlavičku Do Not Track.

9.3.4 Konečné porovnání a zhodnocení

Na základě provedených testů jednotlivých pluginů a jejich funkcí, jak chránit uživatelovo soukromí před sledováním třetími stranami, byla sestavena výsledná porovnávací tabulka. Celkové hodnocení pak bylo sestaveno jako součet bodů na základě bodování podle klíče: 1 bod - splňuje zcela (v tabulce Ano) a 0 bodů – nesplňuje (v tabulce Ne). Nejlépe hodnocen je ten nástroj, který se nejvíce blíží maximu možných bodů (100 % odpovídá maximu možných bodů).

	Ghostery	AdBlock Plus	Privacy Badger
Tracking cookies	Ano	Ano	Ano
Blokace reklam	Ano	Ano	Ne
Hlavička Do Not Track	Ne	Ne	Ano
Otisk prohlížeče	Ne	Ne	Ne
Pixelový tag	Ano	Ano	Ano
Vložené pluginy	Ano	Ano	Ne
Nechtěné přesměrování	Ano	Ano	Ne
Součet bodů	5 ze 7 (71%)	5 ze 7 (71%)	3 ze 7 (43%)

Tabulka 3 - Porovnání nástrojů, které zabraňují sledování uživatelů (zdroj: vlastní archiv autora)

Ve výsledném porovnání se umístily nejlépe pluginy Ghostery a AdBlock Plus. Oba tyto pluginy nabízejí aktivní ochranu uživatele před skrytými sledovacími zařízeními. U Ghostery je třeba trackery blokovat ručně, naproti tomu u AdBlocku jsou blokovány na základě uživatelova seznamu filtrů, který si může sám vytvořit nebo stáhnout. AdBlock Plus je tak více komplexnějším nástrojem především díky neustálému vytváření a aktualizaci nových filtrů. Na druhou stranu očekává AdBlock Plus více uživatelovy iniciativity ve správě těchto filtrů. Plugin Privacy Badger se od výše zmíněných více zaměřuje na uživatelskou přívětivost a jednoduchost. Nabízí tak automatické blokování trackerů, ale i ruční. Oproti Ghostery a AdBlock Plus nabízí možnost neblokovat trackery třetích stran, které dbají na pravidla HTTP Do Not Track hlaviček.

Jako výsledný nejlepší plugin byl tedy vybrán komplexnější AdBlock Plus, který by v kombinaci s Privacy Badgerem nabízel nejlepší možnou ochranu před sledováním. Oba tyto pluginy se nijak neovlivňují a jsou spolu zcela kompatibilní.

10 Závěr

Díky neustálému rozvoji informačních technologií a především internetu je téma digitálních stop čím dál více aktuální a do budoucna tomu tak nejspíše stále bude. Většina uživatelů vnímá svět fyzický a digitální odděleně. Digitálnímu světu však nepřiřazují takovou významnost, jako fyzickému. V dnešní době je však naše digitální identita na stejné úrovni jako fyzická a lze jí stejně tak i zneužít.

Hlavním cílem práce bylo zjistit, jakým způsobem a do jaké míry může uživatel chránit své soukromí před narušením, a to především díky informacím získaným z jeho digitálních stop. Dále pak poukázat na případná rizika a hrozby při zneužití digitálních stop. Kontrola nad stopami aktivními je jednodušší než nad stopami pasivními. Je to proto, že aktivní stopa je utvářena samotným přístupem uživatele. Chránit soukromí si tedy uživatel může sám a to především uvážlivým sdělováním osobních informací, fotografií, komentářů. Oproti tomu nad pasivními stopami nemá uživatel téměř žádnou kontrolu a většinou o jejich zanechání ani neví. Tyto informace sbírají především společnosti třetích stran, které díky nim cílí reklamu na míru každého uživatele. Pro ochranu před pasivními stopami je tedy potřeba použít speciální nástroje.

S ochranou přes pasivními stopami je třeba začít co nejdříve, jelikož vznikají při každém nezabezpečeném pohybu po internetu. Většina uživatelů již tedy po sobě zanechala pasivní stopu. Jak už bylo řečeno, tuto stopu je velmi těžké odstranit. Ochranu nabízí nástroje na odstranění uložených sledovacích souborů. Tuto funkci umožňují i klasické webové prohlížeče, ty však neumožňují odstranění všech typů souborů. Z provedené komparace vybraných nástrojů vyšel nejlépe program CCleaner, který nabízí nejkomplexnější řešení s mnoha funkcemi.

Pokud uživatelé vyžadují vysokou míru ochrany a anonymitu při pohybu internetem, jsou ideálními nástroji síťě Tor, I2P nebo použití webového proxy serveru. Z provedeného porovnávání a testování byl doporučen Tor, který obstál v mnoha funkcích v rámci ochrany uživatelova soukromí.

Posledními nástroji, které se věnují zabránění sledování aktivit uživatele byly v rámci porovnání otestovány webové pluginy Ghostery, AdBlock Plus a Privacy Badger. Všechny tyto programy slouží k zabránění sledování aktivit uživatelů. Z výsledků porovnání byly na základě jejich funkcí doporučena kombinace pluginů AdBlock Plus a Privacy Badger.

Vzhledem k existenci mnoha volně dostupných nástrojů je třeba jejich volbu pečlivě zvážit. Nejlepší míry soukromí lze dosáhnout jejich kombinací, kdy se jejich chybějící funkce doplňují.

11 Seznam použitých zdrojů

6 links that will show you what Google knows about you [online]. Nov 14, 2014 [cit. 2016-03-05]. Dostupné z: https://medium.com/productivity-in-the-cloud/6-links-that-will-show-you-what-google-knows-about-you-f39b8af9decc#.uudbomixj

BITTO, Ondřej. *Rhybaření střídá pharming* [online]. 31. 3. 2005 [cit. 2016-03-05]. Dostupné z: http://www.lupa.cz/clanky/rhybareni-strida-pharming/

BLIZCO, Marek. *Upozornění Google (Google Alerts) nyní k dispozici v češtině a slovenštině* [online]. 15. 6. 2010 [cit. 2016-03-05]. Dostupné z: http://google-cz.blogspot.cz/2010/06/upozorneni-google-google-alerts-nyni-k.html

Centre for the Protection of National Infrastructure. *Tracking my digital footprint: A guide to digital footprint discovery and management* [online]. [cit. 2016-03-05]. Dostupné z: https://www.cpni.gov.uk/Documents/Publications/2015/Digital%20Footprint/10_Tracking%20my%20digital%20footprint_FINAL.pdf

ČERNÝ, Michal. *Digitální stopy* [online]. 19. 9. 2011 [cit. 2016-03-05]. Dostupné z: http://e-bezpeci.cz/index.php/temata/sociotechnika/312-digitalnistopy

ČÍŽEK, Jakub. *Flash prý skrývá nebezpečí, říká se mu Flash Cookies* [online]. [cit. 2016-03-05]. Dostupné z: http://www.zive.cz/clanky/flash-pry-skryva-nebezpeci-rika-se-mu-flash-cookies/sc-3-a-153412/default.aspx

ČÍŽEK, Jakub. *Jak odhalit uložená hesla v Chromu během několika sekund* [online]. 7. 8. 2013 [cit. 2016-03-05]. Dostupné z: http://www.zive.cz/bleskovky/jak-odhalit-ulozena-hesla-v-chromu-behem-nekolika-sekund/sc-4-a-170053/default.aspx

ČÍŽEK, Jakub. *TOR: Skutečně anonymní internet* [online]. 2. 10. 2009 [cit. 2016-03-05]. Dostupné z: http://www.zive.cz/clanky/tor-skutecne-anonymni-internet/sc-3-a-149055/

ČMELÍK, Martin. *TOR (The Onion Router) - systém pro vysoce anonymní a šifrovaný přístup k Internetu*[online]. 18. 4. 2007 [cit. 2016-03-05]. Dostupné z: http://www.security-portal.cz/clanky/tor-onion-router-syst%C3%A9m-pro-vysoce-anonymn%C3%AD-%C5%A1ifrovan%C3%BD-p%C5%99%C3%ADstup-k-internetu

ČTK. *Přibližně každé třetí dítě v Česku má zkušenost s kyberšikanou* [online]. 22.11.2014 [cit. 2016-03-05]. Dostupné z: http://www.denik.cz/z_domova/priblizne-kazde-treti-dite-v-cesku-ma-zkusenost-s-kybersikanou-20141121.html

Digitální vydírání a krádež identity hrozí polovině populace [online]. 15. 10. 2014 [cit. 2016-03-05]. Dostupné z: http://www.securitymagazin.cz/technologie/digitalni-vydirani-a-kradez-identity-hrozi-polovine-populace-1404043253.html

DOČEKAL, Daniel. *Hesla uložená v prohlížeči Chrome lze získat „až překvapivě snadno“* [online]. 7.8. 2013 [cit. 2016-03-05]. Dostupné z: http://www.lupa.cz/clanky/hesla-ulozene-v-chrome-lze-ziskat-az-prekvapive-snadno/

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

Download.cnet: Maintenance & Optimization for Windows [online]. [cit. 2016-03-05]. Dostupné z: http://download.cnet.com/windows/maintenance-and-optimization/?sort=downloadCount~desc

Download.cnet: Web Browsers for Windows [online]. [cit. 2016-03-05]. Dostupné z: http://download.cnet.com/windows/web-browsers/

Easylist [online]. [cit. 2016-03-05]. Dostupné z: https://easylist.adblockplus.org/en/

ECKERTOVÁ, Lenka a Daniel DOČEKAL. *Bezpečnost dětí na internetu: rádce zodpovědného rodiče: Network Security Secrets and Solutions*. 1. vydání. Brno: Computer Press, 2013. 224. str. ISBN 978-80-251-3804-5.

EFF: A privacy-friendly Do Not Track (DNT) Policy [online]. [cit. 2016-03-05]. Dostupné z: https://www.eff.org/dnt-policy

EUROZPRÁVY.CZ. *Google zavádí novou službu: Chcete zamést stopy? Nechte se smazat* [online]. 30. 5. 2014 [cit. 2016-03-05]. Dostupné z: http://veda-a-technika.eurozpravy.cz/internet/94393-google-zavadi-novou-sluzbu-chcete-zamest-stopy-nechte-se-smazat/

Facebook: Stahování informací o vás [online]. [cit. 2016-03-05]. Dostupné z: https://www.facebook.com/help/131112897028467/

FACEMAG.CZ. *Facebook si čte i to, co nechcete sdílet* [online]. 14 12. 2013 [cit. 2016-03-05]. Dostupné z: http://facemag.cz/facebook-si-cte-i-to-co-nechcete-sdilet/

FISH, Tony. *My digital footprint: a two sided digital business model where your privacy will be someone else's business*. London: Futuretext, 2009. 210 str. ISBN 978-095-5606-984.

FIŠEROVÁ, Kateřina. *Spamový filtr* [online]. 30.1. 2015 [cit. 2016-03-05]. Dostupné z: https://www.smartemailing.cz/spamovy-filtr/

Ghostery: Download browser extension [online]. [cit. 2016-03-05]. Dostupné z: https://www.ghostery.com/try-us/download-browser-extension/

Google Inc. *Opt out* [online]. [cit. 2016-03-05]. Dostupné z: https://support.google.com/ads/answer/2662922?hl=en

HALTABUSE.ORG. *Comparison Statistics 2000-2011* [online]. [cit. 2016-03-05]. Dostupné z: http://www.haltabuse.org/resources/stats/Cumulative2000-2011.pdf

HINES, Kristi. *Facebook for Websites: Social Plugins for Your Blog and Business* [online]. [cit. 2016-03-05]. Dostupné z: https://blog.kissmetrics.com/facebook-social-plugins/

HORÁČEK, Aleš. *Nikdy ji neviděl, žena z inzerátu ho i tak zavalila sprostými esemeskami* [online]. 25. 2. 2014 [cit. 2016-03-05]. Dostupné z:

http://usti.idnes.cz/kyberstalking-na-mostecku-zena-ze-seznamky-vydirala-muze-p3c-/usti-zpravy.aspx?c=A140225_105031_usti-zpravy_alh

CHLUPATÝ, Roman. *Digitální stopa: Jak si nezavřít cestu k práci snů? Využívejte sociální sítě s rozumem, radí experti* [online]. 31. 3. 2015 [cit. 2016-03-05]. Dostupné z: http://www.investicniweb.cz/2015/3/31/digitalni-stopa-jak-si-nezavrit-cestu-k-praci-snu-vyuzivejte-socialni-site-s-rozumem-radi-experti/

I2P: Clean installs [online]. [cit. 2016-03-05]. Dostupné z: https://geti2p.net/en/download

Internetový obchod Chrome [online]. [cit. 2016-03-05]. Dostupné z: https://chrome.google.com/webstore/category/apps?hl=cs

IP check [online]. [cit. 2016-03-05]. Dostupné z: http://ip-check.info/?lang=en

JELÍNEK, Lukáš. *(NE) Bezpečný Internet* [online]. [cit. 2016-03-05]. Dostupné z: http://www.borovskeho.cz/zip/nebezpecny_internet.pdf

KASÍK, Pavel. *Microsoft: Pozor, Google čte vaše osobní maily, pojďte radši k nám* [online]. 12. 2. 2013 [cit. 2016-03-05]. Dostupné z: http://technet.idnes.cz/microsoft-proti-googlu-emaily-deb-/sw_internet.aspx?c=A130211_135002_sw_internet_pka

KOTENKO, Jam. *Want to know what data Facebook has on you? A primer on what you get and how to get it* [online]. September 22, 2013 [cit. 2016-03-05]. Dostupné z: http://www.digitaltrends.com/social-media/want-to-know-what-data-facebook-has-on-you-a-primer-on-what-you-get-and-how-to-get-it/

KRATOCHVÍL, Petr. *Anonymní surfování* [online]. 2. 7. 2013 [cit. 2016-03-05]. Dostupné z: http://www.chip.cz/casopis-chip/earchiv/rubriky/technika/anonymni-surfovani/

KRATOCHVÍL, Petr. *Google hacking: cíl zaměřen* [online]. 06.07.2009 [cit. 2016-03-05]. Dostupné z: http://www.chip.cz/casopis-chip/earchiv/vydani/r-2009/chip-06-2009/google-hacking-06-09/

KRATOCHVÍL, Petr. *Vaše stopy na internetu* [online]. 14.07.2011 [cit. 2016-03-05]. Dostupné z: http://www.chip.cz/casopis-chip/earchiv/vydani/r-2011/chip-06-11/stopy-internet/

KREUZIGER, Pavel a Brad CHACOS. *Jak (a proč) surfovat na webu v utajení - 2. díl* [online]. 1. 12. 2012[cit. 2016-03-05]. Dostupné z: http://pcworld.cz/internet/jak-a-proc-surfovat-na-webu-v-utajeni-2-dil-45149

KUNEŠ, Jakub. *Co je sociální inženýrství? - 1. díl* [online]. 02.06.12 [cit. 2016-03-05]. Dostupné z: http://pcworld.cz/internet/co-je-socialni-inzenyrstvi-1-dil-44361

Kybergrooming a Kyberstalking: Metodický materiál pro pedagogické pracovníky [online]. , 34 [cit. 2016-03-05]. Dostupné z: www.ncbi.cz/category/6-metodiky-ucebni-materialy?download=37

Kybergrooming [online]. [cit. 2016-03-05]. Dostupné z: http://www.nebudobet.cz/?cat=kybergrooming

Kyberšikana [online]. [cit. 2016-03-05]. Dostupné z: http://nebudobet.cz/?cat=kybersikana

KYLIÁN, Ivo. *Jak vypnout vtíravé zobrazování určitých reklam Google?* [online]. 4.10.2012 [cit. 2016-03-05]. Dostupné z: http://blog.it-logica.cz/vypnout-zobrazovani-urcitych-reklam-google#.VrYM0FjhDct

MCCLURE, Stuart, Joel SCAMBRAY a George KURTZ. *Hacking exposed 7: Network Security Secrets and Solutions*. USA: McGraw Hill, 2012. 768 str. ISBN 978-0-07-178028-5.

MCMILLAN, Robert. *Spam messages promise Google+ invites, deliver drug ads* [online]. Jul 1, 2011 [cit. 2016-03-05]. Dostupné z: http://www.computerworld.com/article/2509881/security0/spam-messages-promise-google--invites--deliver-drug-ads.html

NEJEZCHLEBOVÁ, Lenka. *I mě zneužil deviant Hovorka. Ten ksicht nezapomenu, vzpomíná žena*[online]. 16. 2. 2009 [cit. 2016-03-05]. Dostupné z: http://zpravy.idnes.cz/i-me-zneuzil-deviant-hovorka-ten-ksicht-nezapomenu-vzpomina-zena-pyv-/krimi.aspx?c=A090213_154133_domaci_nel

NYKODÝMOVÁ, Helena. *Bojíte se krádeže své identity?* [online]. 16. 8. 2006 [cit. 2016-03-05]. Dostupné z: http://www.lupa.cz/clanky/bojite-se-kradeze-sve-identity/

OBR, Jiří. *Sniffing: Odposlech datové komunikace* [online]. 6. 3. 2009 [cit. 2016-03-05]. Dostupné z: http://www.itbiz.cz/sniffing-odposlech-datove-komunikace

Ogilvy: Privacy Policy [online]. [cit. 2016-03-05]. Dostupné z: http://www.ogilvy.com/Privacy-Policy.aspx

Panopticlick: Is your browser safe against tracking? [online]. [cit. 2016-03-05]. Dostupné z: https://panopticlick.eff.org/

PERKINS, Olivera. *More than half of employers now use social media to screen job candidates, poll says; even send friend requests* [online]. May 14, 2015 [cit. 2016-03-05]. Dostupné z: http://www.cleveland.com/business/index.ssf/2015/05/more_than_half_of_employers_no_1.html

Phishing a pharming [online]. [cit. 2016-03-05]. Dostupné z: http://www.bezpecnyinternet.cz/pokrocily/internetove-bankovnictvi/phishing-a-pharming.aspx

PINKAVA, Jaroslav. *Phishing aneb rhybaření 1.* [online]. 26.7.2006 [cit. 2016-03-05]. Dostupné z: https://www.interval.cz/clanky/phishing-aneb-rhybareni-1/

POLESNÝ, David. *Podívejte se, co všechno o vás ví Google* [online]. 9. 3. 2012 [cit. 2016-03-05]. Dostupné z: http://www.zive.cz/bleskovky/podivejte-se-co-vsechno-o-vas-vi-google/sc-4-a-162713/

RAK, Roman a Viktor PORADA. *Teorie digitálních stop a její aplikace v ktiminalistice a forenzních vědách*. Karlovarská právní revue, 2006, č. 4, s.1-21. ISSN 1801-2193

ROZMAJZL, Lukáš. *Jak smazat digitální stopu* [online]. [cit. 2016-03-05]. Dostupné z: http://www.dotyk.cz/14-2014/6_jak-smazat-digitalni-stopu

SIMONITE, Tom. *Facebook's Like Buttons Will Soon Track Your Web Browsing to Target Ads* [online]. September 16, 2015 [cit. 2016-03-05]. Dostupné z: http://www.technologyreview.com/news/541351/facebooks-like-buttons-will-soon-track-your-web-browsing-to-target-ads/#comments

Skipease: The Best People Search Engines [online]. [cit. 2016-03-05]. Dostupné z: http://www.skipease.com/

ŠÍMA, Josef. *Anonymní prohlížení* [online]. 1. 5. 2013 [cit. 2016-03-05]. Dostupné z: http://blog.cibul.cz/2013/05/anonymni-prohlizeni-rychle-spusteni.html

ŠIMEČEK, Martin. *Google Alerts* [online]. 18. 11. 2010 [cit. 2016-03-05]. Dostupné z: http://programujte.com/clanek/2010103100-google-alerts/

TECHCENTRAL. *Digital Footprints* [online]. [cit. 2016-03-05]. Dostupné z: https://www.digitallearn.org/sites/default/files/cop/Your%20Digital%20Footprint.pdf

The Invisible Internet Project (I2P) [online]. [cit. 2016-03-05]. Dostupné z: https://geti2p.net/en/about/intro

Top 50 Ad Agencies [online]. [cit. 2016-03-05]. Dostupné z: http://www.top50adagencies.com/

Tor Browser for Windows [online]. [cit. 2016-03-05]. Dostupné z: https://www.torproject.org/download/download-easy.html.en

W3Schools: Browser Statistics [online]. [cit. 2016-03-05]. Dostupné z: http://www.w3schools.com/browsers/browsers_stats.asp

Webproxy [online]. [cit. 2016-03-05]. Dostupné z: https://webproxy.com/

Whoer [online]. [cit. 2016-03-05]. Dostupné z: https://whoer.net/

ZADRAŽILOVÁ, Iva. *Nebezpečí zneužití osobních informací v době globálního monitoringu s přihlédnutím k možnostem ochrany soukromí. Část II.* [online]. 5. 10. 2009 [cit. 2016-03-05]. Dostupné z: http://www.inflow.cz/nebezpeci-zneuziti-osobnich-informaci-v-dobe-globalniho-monitoringu-s-prihlednutim-k-moznostem-ochr-0

12 Seznam obrázků

13 Seznam tabulek