Anonymita na Internetu

Jakub Skalický

Bakalářská práce
2020

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav informatiky a umělé inteligence

Akademický rok: 2019/2020

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Jakub Skalický**
Osobní číslo:	**A17219**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Softwarové inženýrství**
Forma studia:	**Prezenční**
Téma práce:	**Anonymita na Internetu**
Téma práce anglicky:	**Anonymity on the Internet**

Zásady pro vypracování

1. Zabývejte se pozitivními, negativními a morálními aspekty anonymity na Internetu
2. Jaké informace jsou o uživateli zjistitelné, co všechno poskytuje uživatel serveru.
3. Popište bezpečnostní rizika, úniky informací a bezpečnostní zásady.
4. Popište nástroje pro zachování anonymity na Internetu a demonstrujte jejich implementaci

Rozsah bakalářské práce:
Rozsah příloh:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. KRÁL, Mojmír. *Bezpečný internet: Chraňte sebe i svůj počítač*. Česká republika: Grada Publishing, 2015. ISBN 8024798212.
2. STEVENSON, John. *All you need to know about Darkweb: How to access and what to look out for: How to access and what to look out for*. John Stevenson.
3. BAILEY, Matthew. *Complete Guide to Internet Privacy, Anonymity & Security*. Nerel, 2011. ISBN 3950309306.
4. PETROWSKI, Thorsten. *Bezpečí na internetu: pro všechny*. Liberec: Dialog, 2014, 243 s. Tajemství. ISBN 9788074240669.
5. VANĚK, Jiří, Jiří NOVÁK a David KALIKA. *Jak na Internet bezpečně*. Praha: CZ.NIC, z.s.p.o., 2018, 101 s. CZ.NIC. ISBN 978-80-88168-29-4.

Vedoucí bakalářské práce: **Ing. Lukáš Králík**
Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce: **28. listopadu 2019**
Termín odevzdání bakalářské práce: **15. května 2020**

doc. Mgr. Milan Adámek, Ph.D.
děkan

prof. Mgr. Roman Jašek, Ph.D.
ředitel ústavu

Ve Zlíně dne 9. prosince 2019

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 22. 07. 2020

Jakub Skalický, v. r.
podpis diplomanta

ABSTRAKT

Účelem této bakalářské práce je představit čtenáři Internet jako nástroj, který si vyžaduje obezřetnost při nakládání s osobními informacemi. Práce se snaží seznámit běžného uživatele s různými druhy sledování, varuje ho před možnými úniky dat a naučí jej, jak těmto situacím předcházet. Zároveň se zaměřuje na nástroje bránící soukromí uživatele a zajišťující jeho anonymitu. Práce je konstruována tak, aby byl přechod mezi tématy plynulý a čtenáři tak nabídla co nejpřehlednější postup k dosažení anonymity na Internetu.

Klíčová slova: Anonymita, Internet, Soukromí, Bezpečnost, Sledování, Úniky, VPN, Tor

ABSTRACT

The purpose of this bachelor's thesis is to present the reader the Internet as a tool that requires caution while handling personal information. This thesis tries to introduce an average user to various types of tracking, warns him of possible data leaks and teaches him how to prevent these situations. At the same time it focuses on tools that protect the user's privacy and ensure his anonymity. This thesis is designed in a way, that provides the reader with smooth transition between topics and offers him a clear way to achieve anonymity on the Internet.

Keywords: Anonymity, Internet, Privacy, Safety, Tracking, Leaks, VPN, Tor

Tímto bych chtěl poděkovat panu ***Ing. Lukáši Králíkovi*** za užitečné rady a skvělé vedení při psaní této bakalářské práce. Dále bych chtěl poděkovat mému dobrému příteli ***Matyášovi Mechlovi*** za pomoc s výběrem tématu a neustálou podporu při psaní práce. Chtěl bych poděkovat i mému dobrému příteli ***Justinu Loyovi*** za to, že mi nedovolil studium předčasně vzdát. Nakonec bych chtěl poděkovat ***Bohu*** za to, že jsem na to nikdy nebyl sám.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Málo kdo si dnes umí představit život bez Internetu. Tento nástroj se stal pro lidi velmi důležitý a pro mnoho z nich i zdrojem obživy. Představuje pro člověka svět vědění, zábavy a sociálních interakcí.

Zatím co některé lidi drží při životě, jiní se na něm přiživují trochu jinak. Ať už jde o hackery, společnosti nebo vládu, vždy se najde někdo, kdo bude chtít podstaty Internetu zneužít.

V takovém světě je proto důležitým aspektem anonymita. Anonymita zde nevytváří jen bezpečný prostor, kde se uživatel nemusí bát o svá data a soukromí, ale znamená i svobodu. Anonmita poskytuje všem lidem možnost se otevřít a projevit svůj názor. Záleží na každém, zda toho využije nebo zneužije.

Cílem této práce je seznámit čtenáře s problematikou anonymity na Internetu. V průběhu práce se tedy, kromě historie a vývoje Internetu, čtenář dozví i o pozadí anonymity a jejím etickém aspektu.

V praktické části pak práce čtenáře seznámí s různými způsoby, jak mohou společnosti a stránky uživatele sledovat. Prozradí, na co si dávat pozor. Poučí uživatele o unicích dat a jak zjistit, zda sám nebyl obětí takového úniku nebo čtenáře naučí, jak takovým situacím předcházet a jak se na Internetu pohybovat bezpečně.

Nakonec práce čtenáře seznámí s nástroji, které chrání a poskytují uživateli anonymitu, a to ve formě systémových opatření, nastavení prohlížečů nebo jiného softwaru.

Výstupem by měl být jednoduchý a přehledný návod, který čtenáři představí otázku anonymity na Internetu a poskytne mu postup jak anonymity docílit.

I. TEORETICKÁ ČÁST

1 INTERNET

Internet je pro dnešní společnost velice důležitým nástrojem. Jeho uživatelům slouží jako zdroj vědomostí, prostor pro komunikaci a společenské vyžití, způsob zábavy či zdroj příjmů. Jedná se tedy o všestranný nástroj, bez jehož existence si dnes už mnoho lidí neumí svůj život představit. [1]

V této kapitole se práce zabývá Internetem z pohledu jeho mnoha definic a čtenáři přináší více možností jak jej interpretovat. Taky se zabývá i historií a vývojem tohoto nástroje. Provádí čtenáře od samých počátků Internetu až po některé z předpokladů pro jeho budoucnost, neopomínaje i jeho historii v České republice. Dále se zabývá sociálními sítěmi, jak z dnešního pohledu, tak z pohledu jejich sociologického původu. Nakonec letmo nastíní problematiku deep webu a dark webu.

1.1 Definice Internetu

Definovat Internet není vůbec jednoduché. Existuje více přístupů a způsobů jak Internet interpretovat, z nichž alespoň některé budou v této podkapitole zmíněny.

Internet lze popsat jako decentralizovanou síť spojující různé počítače, která umožňuje sdílení dat, zasílání elektronické pošty a další služby. Také by měla být odolná vůči výpadku jedné nebo několika částí. [2]

Internet může být popsán také jako celosvětová síť počítačů, která obsahuje uložené informace v elektronické podobě a zpřístupňuje je dalším počítačům. Jde o soubor technických prostředků, které umožňují šířit data v jejich elektronické podobě pomocí standardizovaných komunikačních protokolů po celém světě. Měl by zvládat i data, které v době jeho vzniku neexistovala. [1]

Internet se osvědčil i jako prostředek pro spojování lidí. Velice totiž usnadňuje komunikaci mezi jednotlivými uživateli. Umožnil tak vzniku různých komunit lidí, sociálních sítí apod. napříč celým světem. V online prostředí se tak mohou potkat jedinci, kteří možná mají podobné zájmy, ale v reálném životě by na sebe nikdy neměli šanci narazit.

Kromě prostředí pro vznik a navázání nových známostí, vytváří Internet i prostředí ideální pro vznik nových služeb, nových trhů a komerce. Pro mnoho firem znamená i jednoduchou cestu k podnikání v globálním měřítku. [1] [2]

Ze společenského hlediska lze Internetu rozumět i jako informačnímu médiu, které podobně jako noviny, televize, knihy atp., každý den všem uživatelům zprostředkovávají nejaktuálnější informace. [1]

1.2 Historie a vývoj Internetu

Kořeny Internetu sahají až do druhé poloviny dvacátého století, a to konkrétně do roku 1957, kdy Rusko vypustilo první umělou družici Sputnik 1, což bylo pro Spojené státy podnětem k většímu zájmu a investicím do kosmických a vojenských technologií. V tomto období studené války nezbývá USA nic jiného než začít jednat, a tak v roce 1958 ministerstvo obrany Spojených státu agenturu Advanced Research Project Agency (ARPA). Tato agentura se měla zaměřovat na výzkum nových technologií. Roku 1962 je nastartován projekt počítačového výzkumu, jehož úkolem je zajistit správné fungování a provoz armádní sítě v případě, že by byla některá její část vyřazena z provozu. Výsledkem byla na tu dobu unikátní síť bez centrálního uzlu. [3]

Důležitým milníkem pro vývoj Internetu je datum 29. 10. 1969, kdy ve Spojených státech došlo ke spuštění experimentální sítě ARPANET. Síť byla vymezena výhradně pro vládní a vojenské účely. [3]

Roku 1973 se ARPANET rozšiřuje za hranice USA, a to konkrétně do Velké Británie a Norska. Ve stejném roce jsou také položeny základy TCP/IP protokolu, který má později nahradit dosud používaný Network Control Program (NCP). O deset let později, v roku 1983, je od ARPANETu oddělen tzv. Military Network (MILNET), což je separátní vojenská síť. Téhož roku je TCP/IP přeneseno do komerční sféry a jsou položeny základy DNS. K roku 1984 je k ARPANETu připojeno jeden tisíc zařízení. [3]

V roce 1987 vzniká projekt National Science Foundation NETwork (NSFNET). Ve stejném roce se poprvé objevuje i pojem Internet. Roku 1989 se Tim Berners-Lee společně s Robertem Cailliauem vrací k hypertextovým dokumentům a navrhují vývoj World Wide Web (WWW) technologií. Tito pánové pak roku 1991 poprvé zavedli WWW technologie pro potřeby CERNu. První webové stránky pak byly spuštěny 6. srpna roku 1991. Šlo od domovské stránky CERNu na adrese info.cern.ch. [3]

30. 4. 1993 byl vydán dokument, který oficiálně zpřístupnil Internet široké veřejnosti. [3] [4] [5]

1.2.1 Internet v České republice

Historii Internetu by člověk v České republice před rokem 1989 hledal zbytečně, protože tehdejší politická situace zemi bránila v zapojení se do celosvětové sítě. S ústupem komunismu byl pak 13. 2. 1992 na ČVUT poprvé spuštěn Internet v tehdejším Československu. [4]

Současně byl zahájen i projekt Federal Educational and Scientific Network (FESNET), který se zabýval vývojem a výzkumem v oblasti pokročilých síťových technologií. Po rozdělení Československa byla zkratka změněna na CESNET.

Kolem roku 2000 podle statistik překročil počet českých uživatelů Internetu hranici jednoho miliónu. V roce 2012 se pak už jednalo přibližně o 73 % z celkové populace České republiky. [4] [5]

1.2.2 Budoucnost Internetu

Přesto že je vždy těžké odhadnout co se bude v budoucnu odehrávat, lze docela s jistotou říct, že se bude Internet dále vyvíjet, ať už co se týče pokrytí nebo rychlosti, ale i v sociálním a komerčním užití. [3]

Přední výrobce síťového hardwaru, americká společnost CISCO, provedla jeden takový odhad budoucnosti Internetu v roce 2010. Podle tohoto odhadu se předpokládá růst vlivu Internetu v ekonomicky rozvojových zemích. Také odhadují, že lidé narození po roce 1990, kterým se přezdívá „Internetová generace“, si k Internetu vybudují bližší vztah. Dále se předpokládá rozvoj ovládacích prvků. Kromě klávesnice se budou stále více používat gesta, hlas či bio senzory. Celkově se vývoj Internetu bude odrážet na intenzitě rozvoje sítě a technologickém pokroku. Kromě toho bude mít obrovský vliv i přístup uživatelů k nově nabízeným službám a technologiím. Společnost CISCO předpokládá čtyři možné scénáře vývoje. [3] [6]

První z jejich odhadů, lze již v dnešní době pozorovat. Podle společnosti CISCO by se totiž měl Internet stát nedílnou součástí běžného života člověka. Očekávají nárust popularity videí a růst využívání cloudových služeb. [6]

Dalším předpokladem je časem již nebude možno internetovému prostředí důvěřovat. Kybernetické útoky a bezpečnostní rizika budou na denním pořádku a ochrana soukromí a citlivých údajů se stane přiliž nákladnou záležitostí. Upadne komerční využívání Internetu a přednost dostane spíše sociální stránka online světa. [6]

Třetí scénář, poněkud skeptický, ale také reálný, nastiňuje pomalé šíření vlivu Internetu v zemích s dlouhou hospodářskou stagnací. V návaznosti na tuto stagnaci by se tedy dalo očekávat, že uživatelé budou využívat jen některých základních služeb, jako stahování, elektronickou poštu apod. Nebudou se vyvíjet nové technologie a lidé budou Internet používat většinou pro vyhledávání slev a výhodných nabídek. [6]

Poslední z předpokladů říká, že se Internet stane obětí své vlastní popularity. Technologie se nepřizpůsobí rychlému nárustu nových uživatelů a přístup k němu bude značně omezen z důvodu nedostatku IP adres. [3] [6]

1.3 Sociální sítě

Lidé měli odjakživa sklon se stávat členem různých komunit, vést je nebo se s nimi sdílet. Mít obecenství s dalším člověkem tryská přímo z podstaty lidskosti. Celý život jsou lidé součástí komunit jako je rodina, sportovní tým, herecký kroužek atd. Tak to se i ze sociologického hlediska na sociální síť dlouho nahlíželo. [7]

Dnešní chápání sociálních sítí je však odlišné, a to díky příchodu Internetu. Dnes si většina lidí pod tímto pojmem představí nějakou komunitní webovou síť, například Facebook, Instagram nebo Twitter. Takové sítě se zaměřují na sdružování a komunikaci lidí z celého světa, a poskytnutí prostředí, ve kterém se tato komunikace odehrává. Jejich vývoj je popsán níže. [4]

1.3.1 Vývoj sociálních sítí

Pojem „sociální síť“ si dnes mnoho lidí spojuje přímo s Internetem. Málo kdo ale ví, že tento pojem byl zaveden dřív, než byl vůbec zahájen proces vývoje Internetu, jak je popsán výše. Termín jako první uvedl v roce 1954 sociolog Jameson Barnsom, který sociální síť popisuje jako sociální okolí s člověkem v jeho středu. [8]

V druhé polovině dvacátého století toto označení přebírá internetový svět. Počátky sociálních sítí na Internetu byl specifické zejména v používání elektronické pošty. E-mail se v té době kromě komunikace vyznačoval hlavně schopností vytvářet a prohlubovat sociální vztahy. První e-mail byl odeslán 2. 10. 1971, nikoliv však na Internetu, ale na jeho předchůdci, síti ARPANET. [9]

Dalším významným krokem v historii sociálních sítí bylo objevení IRC (Internet Relay Chat), což byl systém pro komunikaci přes Internet v reálném čase. Tvůrcem tohoto tzv. „chatu přes Internet“ byl finský student Jarko Ojkarinnen. [9]

7. 8. 1991 první počítače, elektronická pošta, IRC a další technologie utvořili to, čemu se dnes dá rozumět jako Internet. Toho dne totiž britský vědec Tim Berns-Lee odhaluje světu vůbec první internetovou stránku, čímž obrovskou mírou přispěl k vývoji sociálních sítí do stavu, v jakém jsou je známé dnes. [9]

První projekt, který se podobal dnešním webovým sociálním sítím spatřil světlo online světa roku 1995. Jednalo se o síť Classmates.com vybudovanou Randy Conradem, který je často označován za průkopníka. Tyto webové stránky pomáhaly uživatelům udržovat si vztahy s bývalými spolužáky či spolupracovníky. Tento web funguje do dnes a čítá přibližně 40 milionů uživatelů. [8] [9]

1.4 Dark web

Při běžném užívání Internetu se s velkou pravděpodobností uživatel setkává pouze s malou částí jeho obsahu popisovanou jako „surface web“. Tento povrchový web je často nazýván špičkou ledovce a měl by tvořit pouze přibližných 6 % celkového obsahu Internetu. Celý ledovec pak slouží jako jedna z možností, jak interpretovat Internet. Pod hladinou se skrývají ještě dvě sféry a to tzv.“deep web“ a „dark web“. Ty tvoří zbylých 94 % obsahu. [10]

Deep web (hluboký web), někdy i invisible web, je o úroveň níž, než je povrchový web. Jeho obsah tvoří většinou informace a data, které jsou přístupné pouze pro vyhrazený okruh uživatelů. Typicky se jedná o soubory uležené pod nějakým heslem. Jsou to e-maily, soukromé informace a data, bankovní účty, úřední dokumenty ad. Kromě toho se může jednat i vládní zdroje, akademické informace, právní dokumenty či vědecké zprávy. Hluboký web není přístupný pro běžné uživatele, ale využívá ho vláda, armáda či policie. Přístup k němu není realizován webovým prohlížečem, ale pomocí proxy serveru. [11]

Třetím a nejnižším stupněm Internetu je dark web (temný web) nebo taky darknet, který se dá brát jako část deep webu. Termín dark web se začíná objevovat kolem roku 2009, kdy se rozmáhají nové peer-to-peer (P2P) sítě jako Tor, I2P, Freenet nebo Riffle. Jde o šifrované anonymní sítě, které poskytují vlastní služby a jejichž obsah nepodléhá cenzuře nebo zákonům. Zmiňovaný obsah, který je přístupný pouze se specifickým softwarem, konfigurací nebo oprávněním, je často spojován s protizákonnou a kriminální činností. Je

možno zde najít například různé ilegální obchody, jako obchod s drogami, zbraněmi či dětskou pornografií, ale také hackery, hackerské materiály, politické protesty apod. [11] [12] [13]

2 ANONYMITA

Anonymita je nedílnou součástí dnešní společnosti. V této kapitole se práce zabývá anonymitou z mnoha pohledů. Nejdříve se pozastavuje nad anonymitou jako nad pojmem, tedy rozebírá původ slova, její význam a různá členění. Dále anonymitu rozebírá z historického pohledu. Popisuje různé její podoby od anonymity v literatuře, kultuře nebo politice až po náboženství. Nejdominantnější částí této kapitoly je pak téma anonymity na Internetu. Tato část se zabývá například hnutím Cypherpunk, počátky anonymity na Internetu, soukromím či různými statistickými údaji. Dalším tématem je pak identita a pojmy sní spojené. Na konci této kapitoly se práce pozastavuje nad etickými otázkami anonymity a jejími pozitivními a negativními vlastnostmi. [15]

2.1 Anonymita jako pojem

Slovo „anonymita“ vychází z řeckého „anonymos“, jehož kořeny jsou „an“, zápor a „onoma“, jméno. V doslovném překladu je tedy možno slovu „anonymita“ rozumět jako „bezejmennost“ nebo „bezejmenný“. Obecně lze anonymitu chápat jako utajení totožnosti osoby nebo instituce. Veřejné projevy anonymních subjektů se projevují zejména tím, že původce příslušného výtvoru, činu není obecně znám, případně není vůbec identifikovatelný. [14] [15]

Anonymita může být záměrná i nezáměrná, způsobená buďto osobou, které se týká či někým jiným. Nezáměrnou anonymitu lze najít zejména v historii. Byla způsobena například neúplností historických pramenů nebo třeba faktem, že v určitých společnostech se v té době nepovažovala individualizace některých projevů za příliš podstatnou, a proto nebyla jména autorů uváděna. To se týkalo zvláště uměleckých děl. Motivací záměrné anonymity pak bývají většinou obavy z případných sankcí kvůli překročení určitých společenských standardů nebo pro ochranu vlastního soukromí či soukromí a bezpečí jiné osoby. [15]

Dále může být anonymita dělena na dobrovolnou a nedobrovolnou. Dobrovolná, stejně jako záměrná anonymita, je motivována možnými negativními postihy. Nedobrovolná anonymita může být buď důsledkem přímého donucení nebo jako jediné možné východisko ze situace, kdy je jedinec postaven před rozhodnutí prezentovat se anonymně nebo vůbec. [15]

Jako zvláštní druh anonymity je pak chápána anonymita při pozorování v rámci nějakého sociologického výzkumu. V této spojitosti se pak anonymitě dá rozumět jako respektování

soukromí jednotlivců, kteří jsou součástí výzkumu, či jako garance neidentifikovatelnosti těchto jedinců a garance nakládání se sesbíranými daty pouze v hromadném měřítku. [15]

Častou variantou anonymity je také tzv. „pseudonymita“, kdy se autor, ať dobrovolně nebo ne, rozhodl vystupovat pod nějakou přezdívkou či pseudonymem. Zvláštním typem pseudonymity je pak vydávání se za jinou existující osobu s jinou různou zkušeností a autority. [16]

2.2 Příklady anonymity v historii a dnes

V historii se můžeme setkat s anonymitou různých forem v mnoha okruzích, ať už jde o politickou scénu, kulturu či náboženství.

Hodně často se dá narazit na anonymitu právě v literatuře. Jak je již výše zmíněno, je to způsobeno zejména neúplností historických pramenů nebo faktem, že daná společnost v té době nepovažovala individualizaci za podstatnou. [17]

Dobrou ukázkou první možnosti je například dílo „Epos o Gilgamešovi“, kde se autor bohužel nedochoval. [18]

Jako příklad druhé varianty lze uvést třeba básníka, dramatika a herce Williama Shakespeara, jehož jméno je některými odborníky považováno za pseudonym a pravé jméno údajně není známé, nebo spisovatele Samuele Clemense, který vešel ve známost jako Marc Twain.

Pseudonymitu v historii užívali například i Židé v místech, kde nebyla jejich víra uznávaná. Dále také ženy, které užívaly mužských pseudonymů, aby mohly svobodně vyjádřit svůj názor bez obavy, že ho společnost nepřijme jako rovnocenný.

S určitou anonymitou se také dá dodnes setkat při zpovědi v katolických kostelech, kde je kněz vázán mlčenlivostí. V některých zemích to platí i pro návštěvu lékaře či právníka. [17]

Dnes lze na anonymitou narazit hlavně prostřednictvím internetu nebo médií. Často je možné se v reportážích setkat s rozmazanými obličeji, černými proužky či změnou hlasu, a to zejména z důvodu bezpečí a ochrany svědků nebo důvodů etických

2.3 Anonymita a Internet

Na otázku anonymity se v dnešní kultuře nahlíží zejména ve spojitosti s Internetem. Právě s příchodem Internetu se nastartovala úplně nová éra chápání anonymity jako takové. Tento

její nový, moderní vzhled je často skloňovaným tématem v mnoha sférách a přináší s sebou i mnoho důležitých bezpečnostní, etických a jiných otázek.

2.3.1 Hnutí Cypherpunk

Vůbec první zmínky o polemizování nad otázkou anonymity na internetu lze nejspíše připsat skupině aktivistů zvané „Cypherpunk“. Toto hnutí se začalo formovat přibližně v osmdesátých letech, a jedním ze zakladatelů byla Jude Milhon, hackerka, která ho i pojmenovala. Do obecného povědomí se Cypherpunk dostává se zveřejněním textu Davida Chauma „Security Without Identification: Transaction Systems to Make Big Brother Obsolete.“ Oficiálně pak hnutí vzniká roku 1992. [19] [20] [21]

Příslušníci této skupiny se věnovali bezpečnosti, zejména pak bezpečné komunikaci na internetu. Prohlašují, že jsou odhodláni postavit anonymní systém, a ochraňovat soukromí pomocí kryptografie, které ve svém manifestu, sepsaném Ericem Hughesem, přikládají veliký důraz. „Soukromí v otevřené společnosti také vyžaduje kryptografii.“ „Bráníme naše soukromí pomocí kryptografie, anonymního systému přeposílání pošty, digitálními podpisy a elektronickou měnou.“ [22]

Dalším z cílů skupiny bylo vytvořit anonymní transakce a prosadit elektronickou měnu. Spekuluje se, že za vznik první elektronické měny, Bitcoinu, můžou přímo či nepřímo právě Cypherpunks, kteří prosazovali integraci kryptografie do osobních počítačů a internetu, čímž nastartovali široký zájem o šifrování a jeho vývoj v tomto prostředí. To pak vedlo ke vzniku první veřejné kryptoměny, Bitcoinu. Pravá identita tvůrce Bitcoinu, Satoshi Nakamota, je stále neznámá, ale někteří věří, že jde dost možná o člena Šifropunku. [19] [22]

2.3.2 Počátky anonymity na Internetu

S příchodem Internetu nabývají anonymita a pseudonymita úplně nových rozměrů. Internet nyní poskytuje uživatelům jistou míru pohodlí, se kterou mohou pod určitou anonymitou zasílat zprávy, vystupovat na fórech nebo sociálních sítích, či jednoduše fungovat v jakémkoliv směru v tomto prostředí. Nutno ale podotknout, že Internet byl původně myšlen jako prostředek pro sdílení souborů a informací mezi vzdálenými počítači, nikoliv pro komerční užití či širokou veřejnost. [17] [23]

Otázky identity a identifikace uživatelů se na Internetu objevují až s příchodem komerce do tohoto prostředí a jeho postupně rostoucí sociální stránkou. Na tom má, mimo jiné, podíl hlavně vznik emailových schránek, diskusních fór a později i sociálních sítí. Tyto

komunikační prostředky byly ve většině případů financovány právě reklamou. Pro lepší a cílenější reklamu pak byla vyžadována identifikace uživatelů a jejich osobní informace. Tyto informace vypovídaly o tom, jaký typ obsahu dané uživatele zajímá, a pomáhaly pak autorům získat více návštěvníků, kteří reklamu uvidí. Z důvodu nežádoucímu růstu požadavků na identifikaci, ztrácelo mnoho uživatelů o danou stránku, fórum či službu zájem.

To vedlo k růstu poptávky po alternativním, spíše automatizovaném sběru informací, kde by uživatel nebyl stále nucen k identifikaci. A právě zde lze hovořit o asi prvních náznacích toho, jak se bude otázka anonymity na Internetu vyvíjet. [24]

2.3.3 Soukromí v online světě

Anonymita na Internetu není nikdy stoprocentní. Vždycky je zde možnost, že se daného uživatele nebo predátora podaří vystopovat. To zejména v případě, kdy daný uživatel používá stále stejné metody nabytí anonymity. [17]

Například v případě, kdy uživatel používá nějakou přezdívku nebo pseudonym, neznamená to, že jeho pravá identita není dohledatelná. I přes to, že většina služeb nabízí tvorbu profilu bez nějaké kontroly identity, je možné danou osobu vystopovat pomocí IP adresy (tzv. fyzické adresy). [17]

Během každé relace je uživateli přiřazeno dočasné číslo IP, které je ovšem zapisováno do logů poskytovatelem internetového připojení (anglicky Internet Service Provider, ISP). Tím pádem je možné zjistit, kdo používal danou dočasnou adresu v době, kdy byl vytvořen falešný profil, a tak uživatele identifikovat. [25]

To však není jediné, co je poskytovatel internetového připojení schopen o uživateli zjistit. Poskytovatelé mají také přístup k historii vyhledávání, a to i v případě, že uživatel využije nějakou z anonymních služeb vyhledávání, podporovaných daným prohlížečem. Tato data pak poskytovatel internetového připojení sesbírá a prodá marketingovým společnostem. Někteří dokonce nabízí extra balíčky, či prémiové účty, kde se tomuto sledování může uživatel vyhnout, což je v podstatě jen další z možností, jak vydělat na něčím soukromí. [26]

Řešením může být například využití některé z Virtual Private Network (VPN) nebo proxy serverů, které skryjí IP adresu uživatele a zašifrují veškerou online aktivitu tak, že k nim poskytovatel nemá přístup. U volby VPN a proxy serverů je důležité si dávat pozor na sprostředkovatele této služby, protože i on, stejně jako ISP, může uchovávat nežádoucí, soukromé informace o aktivitách uživatele na Internetu. [17] [25] [26]

Kromě poskytovatelů internetového připojení, mohou uživatelskou aktivitu sledovat například i provozovatelé emailových služeb. Každá emailová hlavička totiž obsahuje i trasu zprávy, která obvykle nebývá v konečné formě uživateli zobrazena. Správce služby si však celou trasu může zobrazit pomocí jednoho příkazu. Příklad takovéhoto trasování je znázorněn na obrázku 1. [17]

```
sentto-1119315-3675-1008119937-jpalme=dsv.su.se@returns.groups.yahoo.com
Received: from n12.groups.yahoo.com (n12.groups.yahoo.com
[216.115.96.62])
by unni.dsv.su.se (8.9.3/8.9.3) with SMTP
id CAA21903 for <jpalme@dsv.su.se>;
Wed, 12 Dec 2001 02:19:32 +0100 (MET)
X-eGroups-Return: sentto-1119315-3675-1008119937-
jpalme=dsv.su.se@returns.groups.yahoo.com
Received: from [216.115.97.162] by n12.groups.yahoo.com with NNFMP;
12 Dec 2001 01:19:00 -0000
Received: (qmail 11251 invoked from network); 12 Dec 2001 01:18:56 -0000
Received: from unknown (216.115.97.167)
by m8.grp.snv.yahoo.com with QMQP; 12 Dec 2001 01:18:56 -0000
Received: from unknown (HELO n26.groups.yahoo.com) (216.115.96.76)
by mta1.grp.snv.yahoo.com with SMTP;
12 Dec 2001 01:18:59 -0000
X-eGroups-Return: lizard@mrlizard.com
Received: from [216.115.96.110] by n26.groups.yahoo.com with NNFMP;
12 Dec 2001 01:12:56 -0000
X-eGroups-Approved-By: simparl <simparl@aol.com> via web;
12 Dec 2001 01:18:15 -0000
X-Sender: lizard@mrlizard.com
X-Apparently-To: web-law@yahoogroups.com
Received: (EGP: mail-8_0_1_2); 11 Dec 2001 20:50:42 -0000
Received: (qmail 68836 invoked from network); 11 Dec 2001 20:50:42 -0000
Received: from unknown (216.115.97.172)
by m12.grp.snv.yahoo.com with QMQP; 11 Dec 2001 20:50:42 -0000
Received: from unknown (HELO micexchange.loanperformance.com)
(64.57.138.217) by mta2.grp.snv.yahoo.com with SMTP;
11 Dec 2001 20:50:40 -0000
Received: from mrlizard.com (IAN2 [192.168.1.119]) by
micexchange.loanperformance.com with SMTP
(Microsoft Exchange Internet Mail Service Version 5.5.2653.13)
id W11PL97B; Tue, 11 Dec 2001 12:53:11 -0800
```

Obrázek 1 – Trasování cesty e-mailu [17]

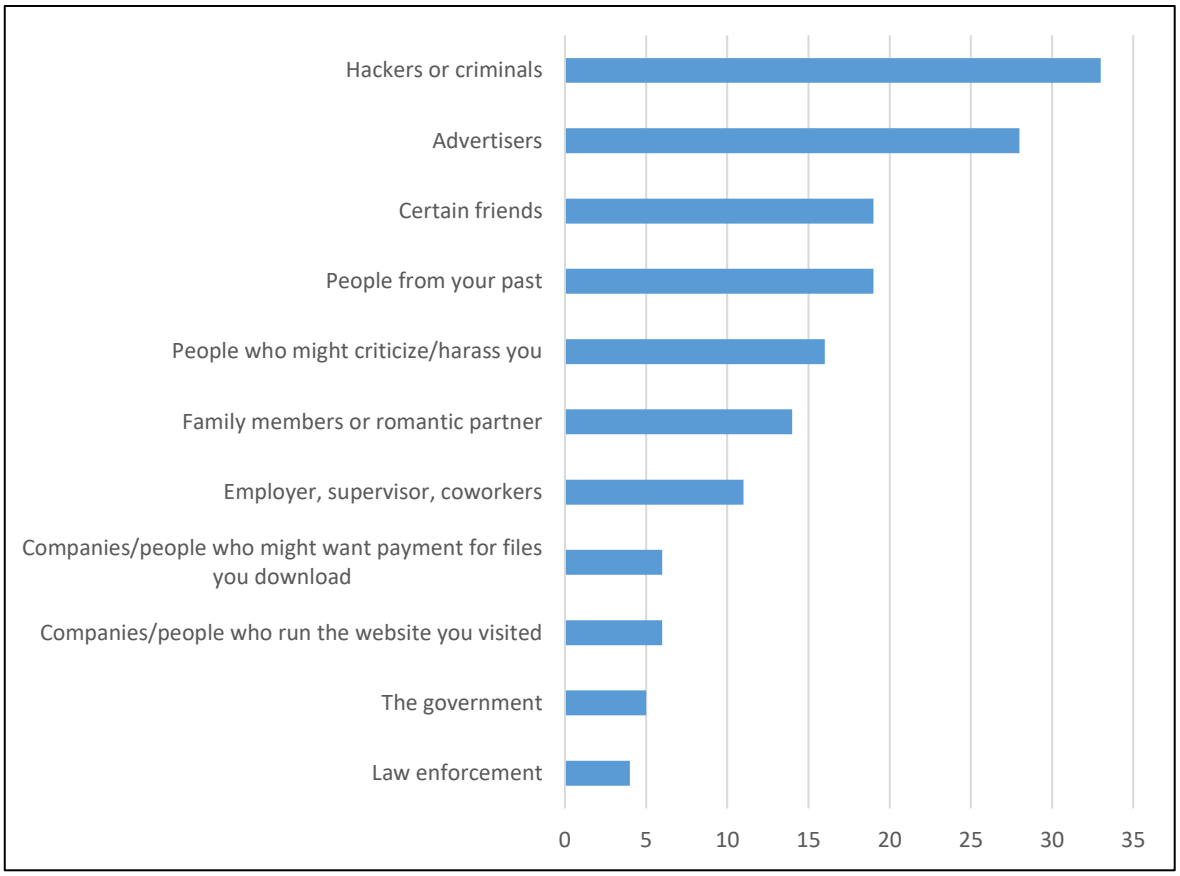
Na obrázku můžeme vidět trasování e-mailové zprávy přes více serverů. Hlavičky jsou postupně přidávány s každou „zastávkou“ se shora. Tudíž původní odesilatel a jeho IP adresa je zobrazena úplně dole, zatímco příjemce zprávy a jeho IP adresy se týká údaj první shora. [17]

2.3.4 Statistiky týkající se online anonymity

Většina internetových uživatelů vyhledávají anonymitu, ale domnívají se, že úplné anonymity dosáhnout nelze. Díky výzkumu z roku 2013, který se zabýval zejména otázkami týkajících se anonymity na Internetu, jsou k dispozici tyto údaje: [27]

- 86 % uživatelů podniklo jisté kroky k zamaskování jejich pohybu a aktivit na internetu
- 55 % uživatelů podniklo kroky k zamezení společností, osob či vlády v omezování jejich soukromí
- 21 % uživatelů mají zkušenost s kompromitováním, či krádeží jejich e-mailových nebo sociálních účtů
- 12 % uživatelů bylo na internetu „stalkováno“ nebo jim bylo vyhrožováno
- 11 % uživatelů přišlo o citlivé soukromé informace
- 6 % uživatelů bylo obětí online podvodů (tzv. scamů) a ztratilo nějaký peněžní obnos
- 6 % uživatelů bylo poškozeno na reputaci po událostech odehraných v prostředí internetu
- 6 % uživatelů na základě událostí odehraných na internetu utrpěli poškozením reputace
- 4 % uživatelů se dostalo do fyzického nebezpečí kvůli něčemu co se odehrálo na internetu

Ze stejného výzkumu čerpal i Daniel Russel ve svém článku „The Anonymity Impossibility: Stats, Surveys, And Figures“ na stránce attentiv.com, kde se zabývá různými otázkami typu: „Proč si lidé cení anonymity?“ nebo „komu se lidé na internetu snaží vyhnout?“. Zejména druhá položená otázka je zajímavá, protože poukazuje na jednu z příčin vyhledávání online anonymity. Podle shromážděných dat se lidé nejčastěji snaží vyhnout hackerům nebo kriminálníkům, a to ve více než 30 %. V těsném závěsu je pak snaha vyhýbat se reklamám, určitým přátelům nebo lidem z minulosti. Nejméně se pak lidé obávají právního vymáhání či vlády viz. obrázek 2. [28]



Obrázek 2 - Komu se uživatelé na Internetu snaží vyhnout [28]

Statistikou využití online anonymity se pak zabývá studie Mikaela Berglunda z roku 1995. Studie je založena na datech, které získal procházením diskusních skupin na švédském serveru Usenet News. Náhodně vybral vždy několik zpráv, které měly anonymního nebo pseudonymního autora a pokusil se zprávu podle obsahu zařadit do určité typové skupiny viz. tabulka 1. Z tabulky je zřejmé, že nejčastějším užitím anonymity, tedy v 30 %, byly diskuse na téma sexu, koníčků, práce a podobně. Dále dominovaly reklamy s erotickým podtextem či otázky a odpovědi na různá témata, a to hlavně z oblasti informačních technologií, nebo se jednalo o témata romantického či erotického rázu. Jako neklasifikované typy zpráv pak uvádí autor takové texty, kterým nebyl schopen porozumět. Většinou se jednalo o zprávy psané v čínštině. Autor se domnívá, že tyto zprávy byly anonymní zejména z politických důvodů, tedy kvůli tamějšího režimu a cenzury s ním spojené. [17]

Tabulka 1 – Využití online anonymity z roku 1995 [17]

Procento	Typ zprávy	Častá témata
30 %	Diskuse	Sex, koníčky, práce, víra, politika, etika, software
23,10 %	Reklama	Reklamy pro navázání sexuálního/romantického kontaktu, hledání přátel s podobnými koníčky
16,50 %	Otázky a odpovědi	Problémy softwarového rázu, počítače, sex, drogy, léky
13,20 %	Text	Erotické texty, vtipy (často nevhodné)
9,90 %	Testovací zprávy	Pro testování anonymity na serveru
3,70 %	Obrázky	Většinou pornografie/erotika
0,40 %	Software	
3,30 %	Neklasifikované	Většinou psané v jazyce, kterému autor nerozuměl. (Např. v čínštině)

2.4 Online identita

Identita uživatele je asi nejdůležitějším aspektem jeho soukromí. Proto je důležité znát jakým způsobem může být jeho anonymita na Internetu narušena, a které vlastnosti jeho identitu v tomto prostředí popisují. Tato podkapitola se tedy zabývá tzv. identifikačními informacemi a také technologiemi, které tyto informace mohou o uživateli zjistit. [30]

2.4.1 Identifikační informace

S anonymitou na Internetu je úzce spojena i otázka toho jakým způsobem jsou osoby na v online prostředí identifikovány, a co vlastně tvoří identitu online uživatele. Toto téma je pro soukromí uživatelů velice podstatné, protože jejich anonymita přímo závisí na schopnosti co nejlépe zamaskovat právě ty informace, které je mohou identifikovat. Jedná se o tzv. „Identifikační informace“ a patří mezi ně následující:

- Jméno osoby
- Lokace
- Pseudonym spojitelný s reálným jménem nebo lokací
- Pseudonym prozrazující jiné informace
- Odhalující vzorce chování
- Členství v některé sociální skupině

- Informace, předmět či dovednost naznačující osobní charakteristiky

Jednotlivé položky na tomto seznamu se mohou zdát samostatně celkem nic neříkající, ale v kombinaci jedné s druhou můžou tyto informace vést k nabourání anonymity uživatele a jeho soukromí. Tato sedmička identifikačních informací je jeden ze způsobů, jak se mohou například i obyčejní Internetoví uživatelé dopátrat reálné osoby, která na Internetu vystupuje pod nějakým pseudonymem, pouze pomocí intuice a pozorování. Anonymita uživatelů se tak stává obětí jejich vlastní neuváženosti a nepozornosti, na které je bohužel krátké jakékoliv softwarové zabezpečení. [29] [30]

2.4.2 Identifikační technologie

Když je pominut lidský faktor, tedy neopatrnost a nedbalost při vystupování v online světě, je pro anonymitu uživatele nebezpečný zejména software. Dnešní moderní technologie poskytují mnoho způsobů, jak uživatele identifikovat. [29]

Kromě IP adresy, o které je již výše zmínka, jsou nebezpečné i technologie určování polohy. Geolokace a podobné techniky dokáží dnes určit polohu zařízení s přesností až na jeden metr. Jako příklad takové technologie může být uvedena třeba Constraint-based geolocation, která je schopna aktivně měřit vzdálenost na základě odezvy. S určováním polohy se, ale uživatelé denně setkávají také u mobilních zařízení, kde je tato služba zprostředkována pomocí GPS. GPS je velmi užitečný nástroj, který se může v některých situacích zdát nedocenitelný. Na druhou stranu dnes přibývá aplikací, které vyžadují přístup k této službě, což pak může znamenat potencionální riziko odhalení polohy a dalších informací o uživateli. [29]

Poloha subjektu může být však zjištěna i jinými, kreativnějšími způsoby. Jedním takovým je kupříkladu obsahová analýza příspěvků na webu. Analýzou veřejně přístupných dat, poskytnutých uživatelem, lze odhadnout lokaci této osoby. Jedná se o údaje od názvů států, měst, restaurací a jiných míst v příspěvku, až po aktivitu uživatele, tedy například časy přidávání příspěvků, podle kterých se dá určit třeba časová zóna. [29]

Mezi další identifikační technologie patří tzv. „cookies“. Jsou to krátké textové soubory, uložené v počítači uživatele, které vytvořil webový prohlížeč za účelem pozdějšího znovunabytí dříve získaných informací. Je to způsob, jakým je prohlížeč schopen si pamatovat různé informace, které mu pomohou uživatele jednodušeji identifikovat nebo na

něj lépe a efektivněji cílit reklamu. V praxi se může také projevit předvyplňováním přihlašovacích údajů, což je v určitém ohledu velké usnadnění a šetření času, nebo hraje i podstatnou roli na e-shopech při vkládání zboží do košíku. [29] [31]

2.5 Etické aspekty anonymity na Internetu

Anonymní vystupování v online prostředí je velice kontroverzní téma. To, co by mělo přinášet bezpečí a svobodu slova, může přinést i skepsi, strach a emoční, popřípadě i fyzickou, bolest. Vždycky se najdou tací, kteří budou možnosti se svobodně vyjadřovat zneužívat. Fakt že takto mohou činit v podstatě bez následků, celé věci akorát přidává na vážnosti. V této podkapitole jsou zmíněny jak pozitivní, tak i negativní vlivy anonymity na společnost v prostředí Internetu. [32]

2.5.1 Pozitivní vlastnosti

Anonymita na Internetu poskytuje uživatelům svobodu slova a volnost se vyjadřovat beze strachu, že by jejich názor mohl ovlivnit jejich sociální postavení či jim jiným způsobem ublížit.

Také umožňuje vzniku svědectví lidí, kteří si prošli určitou negativní či traumatickou situací, ať už se jedná o závislosti, nemoci nebo smrt blízkého atp., a přispět tak svými zkušenostmi k podpoře lidí, kteří si podobnou situací možná právě prochází. Často jde i o témata, které je těžké s někým osobně sdílet, proto daná osoba raději zvolí anonymní přístup.

Dále anonymita představuje svobodu projevit své politické názory, a to i v zemích, kde jsou za ně lidé pronásledováni. [17]

Lidé se také mohou dočkat více objektivních reakcí na jejich názor, když nepoužijí své vlastní jméno. Uživatelé jsou si více rovni a faktory jako věk, národnost, víra nebo barva pleti apod. neovlivní jejich postavení v diskusi.

Anonymita na internetu je také důležitá například pro sociální experimenty, elektronickou měnu, zabezpečení citlivých dat atd. [17] [32]

2.5.2 Negativní vlastnosti

Anonymita na Internetu samozřejmě přináší i mnoho negativních aspektů. Jedním z nich je toxické chování a nevhodné komentáře některých uživatelů. Mnoho lidí na Internetu se nebojí říct to, co by v reálném světě neřekli, protože jsou chráněni právě anonymitou.

Nikomu se za své chování nemusí nikomu zpovídat nebo nést nějaké následky. To je jeden z důvodů proč se rasizmus a kyberšikana na Internetu tak často objevují. [32]

Anonymita může být také zneužita k nezákonným činnostem jako podvody, vyhrožování, stalkování, šíření virů, šíření dětské pornografie apod.

Anonymita v online prostředí může být také nebezpečná pro mladší uživatele, zejména děti a teenagery. Často totiž mohou narazit na tzv. „predátory“, kteří z nich mohou vymanit různé citlivé informace či jakékoliv materiály, které jsou později použity k vydírání. Neškodná konverzace s anonymním uživatelem tak může vést až k fyzickému násilí a pedofilii. [32] [33]

Anonymita na Internetu může napáchat mnoho škody. Nejen na Internetu, ale i v běžením životě by přitom stačilo kdyby se lidé inspirovali myšlenkou zapsanou v Bibli v Evangeliu Lukáše 6, 31: „Jak chcete, aby lidé jednali s vámi, jednejte i vy s nimi.“ [34]

PRAKTICKÁ ČÁST

3 SOUKROMÍ NA INTERNETU

Uživatelé za sebou při procházení Internetem zanechávají digitální stopu. Toho pak využívají různé společnosti a webové stránky, aby mohli vést lépe cílené reklamy ušité na míru jednotlivým uživatelům. Tento typ informací může však často být velmi citlivý či osobní. [35]

Kdo může uživatele sledovat a co všechno je o něm zjistitelné? Jak poznat, zda došlo k úniku informací? Jaké jsou bezpečnostní zásady a jak by se měli uživatelé na internetu chovat? Na tyto a další otázky se pokusí práce v této kapitole, co možná nejsrozumitelněji, odpovědět.

3.1 Sledování uživatele

Jak už bylo výše zmíněno, uživatel za sebou při procházení Internetem zanechává tzv. digitální stopu. Poskytuje tak různým společnostem a webovým stránkám informace, které pak mohou legálně shromažďovat a využít například k cílenému marketingu. Jedná se o data jako lokace, typ zařízení, stav baterie, používaný prohlížeč nebo historie vyhledávání a aktivita daného uživatele. [35] [36]

3.1.1 Cookies

Hlavním zdrojem obživy pro tyto nenasytné webové stránky jsou soubory cookies (sušenky). Jde o malé množství dat, které server sesbírá a předá počítači. Existují dva druhy. Zatím co dočasné soubory cookies trvají jen danou relaci, trvalé soubory cookies jsou uložené v počítači a nejsou po zavření prohlížeče vymazány. Při opětovném otevření prohlížeče pak počítač zasílá tato data zpět serveru. [37]

Tolik tedy k tomu, jak cookies fungují. Ale proč jsou vlastně špatné? V podstatě nejsou samy o sobě zlé. Původní myšlenkou bylo uživateli ulehčit práci. Mezi takové cookies patří třeba tzv. „authentification cookies“ (autentifikační cookies), které se starají o automatické vyplňování formulářů. To však jiným může znít až děsivě. V tomto případě jde o osobní preference.

Hlavním negativním prvkem souborů cookies je však fakt, že slouží jako registr aktivit uživatele, na jehož základě mohou různí prodejci lépe cílit svou reklamu. [26]

O tom, jak se tomuto ohrožení bránit pojednává práce více v kapitole „Nástroje pro zachování anonymity“, konkrétně v podkapitole „Nastavení prohlížeče a užitečné doplňky“.

3.1.2 IP adresa a odhalení polohy

Některé informace jsou webovým stránkám poskytovány nehledě na nastavení prohlížeče. Mezi takové informace patří IP Adresa, kterou počítač sdílí okamžitě co je online. Ta je většinou klíčová k odhalení polohy zařízení. [38]

Toho využívá například Google k sestavení podrobné časové osy pohybu uživatele. Takto má Google přístup k informacím kde a kdy se uživatel nacházel.

Časová osa je přístupná v aplikaci Google Maps. Stačí kliknout na tlačítko „nabídka“ a v menu zvolit možnost „Vaše časová osa“. Objeví se mapa s vyznačenými lokalitami, které daný uživatel navštívil v určitém časovém úseku. Časový úsek lze přizpůsobit pomocí nabídky v levém horním rohu. [38]

Funkci je možné vypnout po kliknutí na ozubené kolečko v pravém dolním rohu mapy, a zvolení možnosti „pozastavit historii polohy“. Podle výzkumu portálu APNew.com, ale není uživatel ani tak ušetřen sledování tímto informačním gigantem. [39]

Řešením tak může být třeba VPN, jehož implementace je popsána dále v této práci.

3.1.3 Co může sledovat poskytovatel připojení

K soukromí uživateli nepomůže ani oblíbený anonymní režim. Ten sice zamezí ukládání historie v prohlížeči a po jeho zavření smaže nové cookies soubory, ale poskytovatel internetového připojení (anglicky Internet Service Provider, ISP) data o aktivitách uživatele na Internetu k dispozici má. Ten je může legálně shromažďovat a dále prodávat. Mezi takové informace patří například:

- Profil uživatele, kdo je
- Kdy byl uživatel online, aktivní
- S kým uživatel komunikoval
- Co uživatele zajímá, co vyhledává

Tyto informace, v kombinaci s daty sesbíranými pomocí souborů cookies nebo metodou fingerprinting, mohou společně vést k sestavení velmi detailního profilu internetového uživatele. [40] [36]

3.1.4 Skripty

Mezi další rizika narušení anonymity uživatele patří často používané skripty. Stejně jako soubory cookies i skripty byly vytvořeny s dobrým záměrem. Pomáhají stránky oživit a přináší mnoho funkcionalit, které vytvoří jedinečné a příjemné prostředí pro jejich uživatele. Samozřejmě ne všechny jsou prospěšné. Skripty vytvořené se zlým úmyslem často zneužívají bezpečnostních děr v programech a snaží se tak infikovat počítač škodlivým malwarem. [37]

Jedním ze škodlivých skriptů je tzv. exploit (vytěžení). Ten využívá bezpečnostních mezer k propašování škodlivého obsahu, malwaru. Toto se dá řešit včasnými aktualizacemi, které ošetří jednotlivé díry v systému nebo programu.

Dalšími nebezpečnými skripty jsou například hijacker (únosce) a sniffing (čmuchání). Hijacker mění adresy webových stránek. Může se tak stát, že je uživatel přesměrován na nežádoucí stránku. Sniffing je zase technika, při níž jsou ukládány a následně čteny TCP pakety. Používá se zejména při diagnostice sítě či odposlechu datové komunikace. Útočník tak může získat potřebná data nebo i hůř, proměnit napadený počítač v odposlouchávací stanici. [37]

3.1.5 Fingerprinting

Málo známá, přes to velmi účinná a přesná metoda identifikace unikátních prohlížečů je fingerprinting. Metoda je postavena na faktu, že zařízení a prohlížeče mohou za sebou na Internetu zanechávat tzv. fingerprints (otisky). Jedná se o informace sesbírané o vzdáleném zařízení za účelem jeho identifikace. Tato metoda může spolupracovat se soubory cookies, ale je na nich také zcela nezávislá. Tedy je možné uživatele nebo zařízení identifikovat i v případě, že jsou soubory cookies deaktivovány. [41]

Kdykoliv se tak uživatel připojí na Internet, předává serveru spoustu informací o stránkách, které navštěvuje a ne jen to. Fingerprinting sesbírá i data o typu prohlížeče, jeho verzi a používaných addonech, operačním systému, časové zóně, jazyku, dokonce i o rozlišení obrazovky a mnoho dalších.

Tato data se mohou zdát zprvu docela náhodná, ale jejich kombinací vzniká jedinečný otisk. Podle výzkumu je šance, že se budou otisky dvou prohlížečů shodovat ve 100 % asi 1 ku 286 777 prohlížečům. [41]

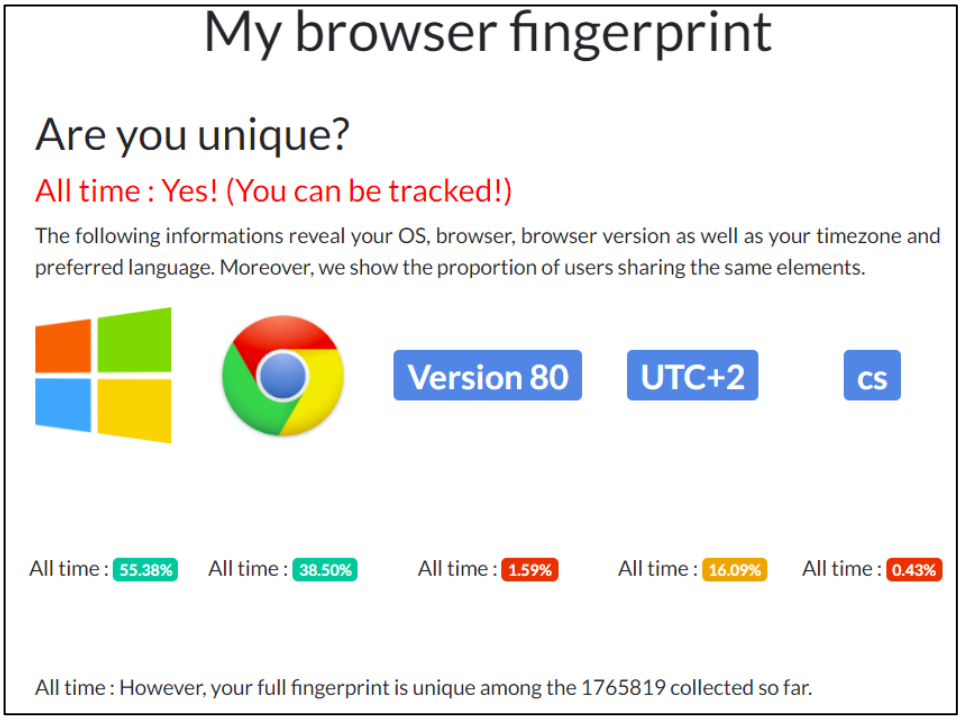
Existuje hned několik nástrojů, které uživateli pomůžou otestovat identitu jejich prohlížeče.

3.1.6 Am I Unique

Tento nástroj si pokládá za cíl prozkoumat rozmanitost otisků prohlížečů (browser fingerprints) a poskytnout pak uživatelům a vývojářům data, které přispějí k vytvoření účinné obrany proti tomu a jiným druhům sledování. Jedná se o komplexní seznam několika atributů, tzv. datových bodů, mezi které patří například informace, zda jsou povoleny soubory cookies či jsou blokovány, jakou platformou uživatel disponuje, typ prohlížeče včetně verze a typ zařízení. [41] [42]

Nástroj je velmi jednoduché použít. Uživatel si nejprve otevře webovou stránku **amiunique.org**[1]. Tam na něj bude čekat tlačítko „View my browser fingerprint“. Po kliknutí služba sesbírá jeho prohlížečový otisk.

Dále se zobrazí výsledky sesbírané tímto nástrojem. U testovacího subjektu výsledky prozradily, že je jeho otisk unikátní. Mezi 1 765 819 sesbíranými otisky, se jeho otisk s žádným ve 100 % neshoduje, tudíž může být snadno sledován. Kromě toho také výsledky správně uvedly použitý operační systém a prohlížeč, jeho verzi, časové pásmo a upřednostňovaný jazyk. V detailnějším přehledu se pak nacházely další atributy, které ovšem pro běžné uživatele nemají takovou informační hodnotu, jako ty již dříve zmíněné. [42]



Obrázek 3 – Výsledky sesbírané nástrojem Am I Unique [42]

[1] https://amiunique.org/

3.1.7 Panopticlick

Dalším šikovným nástrojem pro otestování otisku prohlížeče je **Panopticlick**. Jedná se o výzkumný projekt nadace Electronic Frontier Foundation, který uživateli odhalí, jak účinně je schopen se sledování bránit.

Testování je opět velmi jednoduché. Stačí si načíst stránku **panopticlick.eff.org**[2] a kliknout na tlačítko „TEST ME“. Po chvíli se dostaví výsledky.

Prohlížeč testovacího subjektu se prokázal, jako schopný v blokování sledovacích reklam, ale už nebyl schopen blokovat neviditelné sledovače nebo uživatele ochránit před fingerprintingem (metoda sběru otisků prohlížeče). [41] [43]

Test	Result
Is your browser blocking tracking ads?	✓ yes
Is your browser blocking invisible trackers?	✗ no
Does your blocker stop trackers that are included in the so-called “acceptable ads” whitelist?	✓ 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 4 - Výsledky sesbírané nástrojem Panopticlick [43]

Po kliknutí na „Show full results for fingerprinting“ (zobrazit všechny výsledky sběru otisků) se zobrazí další sesbírané informace, jako například fakt, že mezi 172 503 testovanými prohlížeči je otisk prohlížeče subjektu jedinečný. Dále lze v rozšířeném přehledu najít například typ a verzi prohlížeče, časovou zónu, jazyk, platformu nebo dokonce i velikost paměti RAM zařízení. [43] [37]

[2] https://panopticlick.eff.org/

3.1.8 Privacy.net

Poslední nástroj, kterým se práce v této podkapitole zabývá, je **Privacy.net**. Ten pomáhá uživateli odhalit, jaké informace poskytuje webovým stránkám.

Uživatel si nejprve načte stránku **privacy.net**[3]. Pak stačí kliknout na tlačítko „START TEST“. Poté nástroj projde uživatelův prohlížeč a sesbírá potřebná data. Tato akce potrvá pár vteřin. Poté se objeví výsledky.

U testovacího subjektu nástroj provedl hned několik testů. Nástroj odhalil informace jako IP adresa, poskytovatel internetového připojení, přibližná lokace, typ prohlížeče a verze či informace o zařízení jako typ, operační systém nebo stav baterie. Další testy správně uvedly používané služby a účty na sociálních sítích nebo fakt, že je uživatel vystopovatelný pomocí fingerprintingu. [44] [37]

3.2 Úniky informací

V předchozí kapitole práce nastínila, jak může internet sledovat jednotlivé uživatele. Jednalo se o velmi individuální přístup sledování, pomocí IP adres, souborů cookies, skriptů či unikátních otisků prohlížeče. To však není jediné riziko, se kterým se anonymita uživatele musí v online světě potýkat. Další možností, jak se mohou soukromá data uživatelů dostat do rukou nesprávných lidí jsou pak úniky dat. [45]

Různé webové stránky, online bankovnictví, e-shopy a podobně, jsou dnes vystaveny riziku kybernetických útoků. Zde už hraje obezřetnost uživatele menší roli a hodně záleží na zabezpečení, kterým disponuje strana poskytující danou službu. [45]

Takovýchto útoků stále přibývá. Důvodem mohou být zlepšující se schopnosti útočníků, ale i nedbalost společností. Ta se projevuje buď nedostačujícím zabezpečením nebo selháním lidského faktoru, například nechtěné sdílení citlivých dat. A takové případy opravdu existují.

V této podkapitole se práce bude zabývat právě úniky dat. Nabídne příklady některých z největších úniků informací dnešní doby, stejně jako možnost, jak může uživatel zjistit, zda se ho některý z úniků netýká. [45] [46]

[3] https://privacy.net/analyzer/

3.2.1 Největší úniky dat

Útokům či občasné nedbalosti se nevyhnou ani velké společnosti. Příkladem toho může být incident z roku 2013, kdy společnost Adobe přišla o údaje přibližně 153 miliónů uživatelů. První vyjádření firmy zahrnovalo zprávu o 3 miliónech zcizených zašifrovaných údajích o kreditních kartách. Později vyšlo najevo, že firma přišla o 153 miliónů jmen, hesel a informací spojených s kreditními a debetními kartami. [46]

V roce 2014 zase firma eBay zveřejnila zprávu, že došlo k odcizení jejich celého seznamu účtů. Jména, adresy či data narození asi 145 miliónů zákazníků padly do rukou útočníků. Podle společnosti eBay útočníci využili přihlašovacích údajů třech z jejich zaměstnanců a měli tak po dobu 229 dní přístup k celé jejich databázi. [46]

Za zmínku stojí také firma LinkedIn, která v letech 2012 a 2016 přišla o informace cca 165 miliónů účtů, nebo společnost Yahoo, která ztratila kontakty a citlivé údaje přibližně 3 miliard uživatelů mezi lety 2013 a 2014. [46] [47]

3.2.2 Have i been pwned

Skvělý způsob pro zjištění, zda byl některý z účtů uživatele zkompromitován během některého z datových úniků, je nástroj „Have i been pwned“. Ten momentálně obsahuje údaje o únicích z 437 napadených stránek, což představuje přibližně 9,5 miliard zkompromitovaných účtů. [48]

Použití je velmi jednoduché. Nejprve si uživatel otevře webovou stránku **haveibeenpwned.com**[4]. Poté už stačí jen zadat e-mailovou adresu účtu, který má být ověřen, a kliknout na tlačítko „pwned?“.

Bez jakéhokoliv čekání je uživatel seznámen s výsledky. Nejdříve se objeví hláška, zda byl účet objetí některého z úniků či nikoliv a dále následují doporučení pro lepší ochranu uživatelských údajů. Nakonec si uživatel může prohlédnout seznam webových stránek, u kterých se buď zaregistroval nebo jim jiným způsobem propůjčil své osobní údaje, načež byly tyto stránky či společnosti oběťmi hackerského útoku nebo lidského pochybení, čímž došlo ke kompromitaci uživatelských informací. [48]

[4] https://haveibeenpwned.com/

U osmi z desíti testovacích subjektů došlo ke kompromitaci.

Obrázek 5 - Výsledek nástroje Have i been pwned [48]

3.3 Bezpečné chování na Internetu

Jedním ze způsobů, jak předejít krádeži identity nebo zcizení citlivých údajů a osobních informací je určitě obezřetnost a morální kodex.

V této podkapitole se práce zabývá internetovou etikou, bezpečnostními zásadami v online světě, způsoby, jak si zvolit silné heslo, a podobně. [49]

3.3.1 Internetová etika

Internet je mimo jiné i prostředkem pro spojování a komunikaci lidí. Ovšem fakt, že nedochází k fyzickému setkání, ale pouze virtuálnímu, přidává některým jedincům na kuráži se chovat vůči ostatním uživatelům nedůstojně či vulgárně. Tito jedinci mohou případně projevit snahu uživatele obrat o citlivé informace a ty následně využít k jejich diskreditaci nebo je jinak poškodit. Kdyby se však všichni řídili následujícím etickým kodexem, bylo by mnoho bezpečnostních opatření zbytečných. [49]

Netiketa:

- Uživatel by se měl chovat slušně
- Uživatel by se měl snažit řídit pravidly, které platí pro toho, s kým komunikuje a akceptovat kulturní rozdíly.
- Uživatel by měl tolerovat chyby při komunikaci
- Uživatel by měl respektovat soukromí ostatních uživatelů
- Uživatel by měl mít porozumění a toleranci vůči technicky méně zdatným jedincům
- Uživatel by neměl záměrně rozesílat spam, reklamu, hoaxy či malware apod.
- Uživatel by neměl porušovat autorská práva

Další etické zásady lze najít na webu hoax.cz[5]. [49] [37]

3.3.2 Zásady bezpečného vystupování v online světě

Je třeba vzít v úvahu fakt, že zde vždy budou jedinci, kteří své anonymity budou zneužívat, či se naopak snažit nabourat anonymitu jiných. Z toho důvodu je dobré vědět, jak těmto útokům předejít a jak být v internetovém prostředí obezřetný. [50] [51]

Jednotlivé zásady byly seskupeny do bodového seznamu pro větší přehlednost:

- Správa hesel. Je důležité mít silná hesla a pravidelně je měnit. (heslům je věnován odstavec níže)
- Dobrou zásadou je také neodpovídat pravdivě na bezpečnostní otázky. Pro útočníka totiž může být jednoduché zjistit jméno matky za svobodna apod.
- Doporučuje se využívat dvoustupňového zabezpečení. To je takové, které požaduje kromě hesla i například kód, který přijde uživateli na telefon nebo e-mail. Pokud tuto možnost daná služba nabízí je dobré toho využít.
- Důležité je také se připojovat pomocí HTTPS, a to zejména v případech, kdy dochází k přenosu citlivých dat, například při bankovnictví nebo v e-shopech atd. Protokol HTTPS je bezpečnější variantou HTTP a dokáže šifrovat přenos dat.
- Další vhodnou zásadou je používat neveřejný e-mail, pro přihlašování do citlivých služeb jako je bankovnictví. Jde o e-mail, který zná jen jeho uživatel a nepoužívá jej k běžné komunikaci. (problematice e-mailů se práce více zabývá v odstavci níže)
- Doporučuje se také promazávat historii a cache paměť nebo neukládat hesla do prohlížeče. Pokud by se totiž útočník dostal k počítači uživatele, který si hesla ukládá a historii nemaže, stačila by mu základní znalost jazyk HTML a CSS a hesla by získal. Kromě toho by měl i přístup ke všem stránkám, které daný uživatel na Internet navštívil.
- Je vhodné používat inkognito/anonymní režim. Je ale dobré vědět, že uživatele nechrání před fingerprintingem nebo sledování ze strany ISP.
- Je vhodné používat dalších nástrojů pro anonymizaci a bezpečnost, jako je VPN či různé prohlížečové pluginy. (viz. Kapitola „Nástroje pro zachování anonymity“)

[5] https://www.hoax.cz/hoax/netiketa

- Důležité je také udržovat prohlížeč a operační systém aktualizovaný. S aktualizacemi totiž přichází i ošetření možných slabin, které by mohli hackeři či malware využít. [50] [51] [52]

3.3.3 Hesla

Asi nejdůležitějším aspektem soukromí a anonymity jsou hesla. S technologickým vývojem jsou dnes zařízení schopná slabá hesla uhádnout i metodou brute force attack (útok hrubou silou) během chviličky. [26]

Heslo by tedy nemělo být přiliž lehké, uhodnutelné nebo odvoditelné. Nemělo by být krátké nebo jednoznakové (jenom písmena A-Z nebo jenom číslice 0-9). Hesla by se měla pravidelně měnit a pro každou službu být odlišné. Také by je uživatel neměl ukládat v prohlížeči nebo někde jinde, kde nejsou dobře chráněná.

Doporučují se hesla s více než osmi znaky, kde se budou střídat velká a malá písmena, číslice a speciální znaky. [26]

Skvělý nástroj na ověření síly hesla je **howsecureismypassword.net**[6]. Zde stačí vepsat své heslo a nástroj prozradí, jak je bezpečné a jak dlouho by trvalo jej uhádnout. [53]

Obrázek 6 - Výsledky nástroje howsecureismypassword.net [53]

[6] https://howsecureismypassword.net/

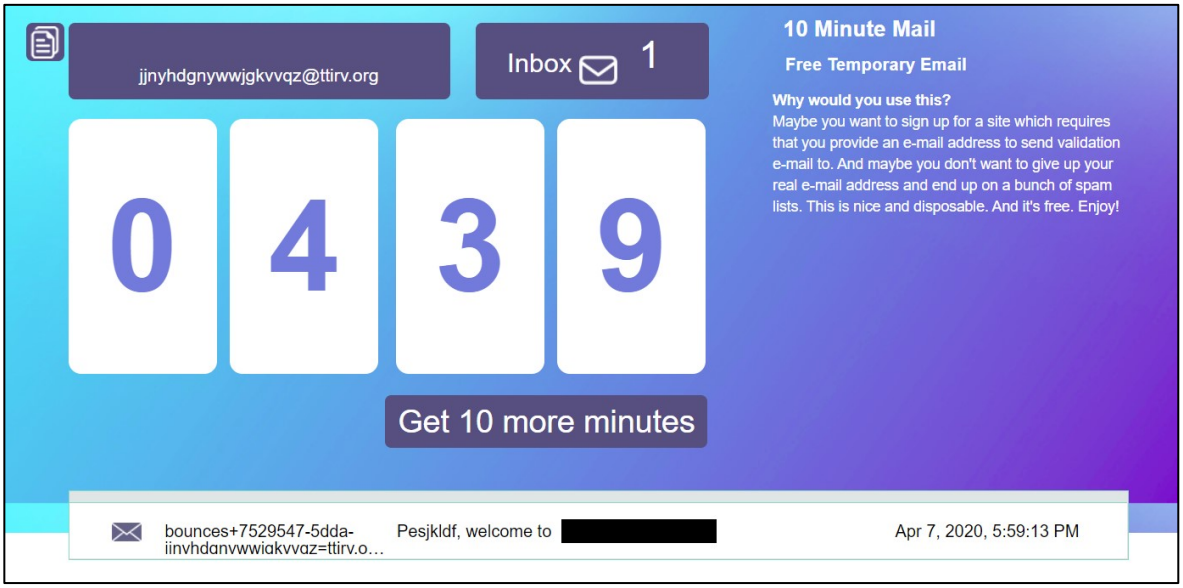
Dobré je taky používat nějaký program pro správu hesel (klíčenku). Vhodný je například nástroj **Dashlane**[7] nebo **1Password**[8]. Z neplacených nástrojů pak třeba **Bitwarden**[9]. [54]

3.3.4 E-maily

Dnes jsou e-mailové adresy velmi často používány jako jeden z přihlašovacích údajů. Je proto důležité, aby byl uživatel opatrný v tom, jak s nimi nakládá.

Jak už bylo výše zmíněno, pro citlivé služby jako bankovnictví je vhodné mít tajný e-mail, který uživatel nepoužívá pro běžnou komunikaci. V případě, že jde naopak o pochybnou službu je dobré zase nepoužívat ani e-mail určený pro běžnou komunikaci. V tomto případě je vhodný velmi šikovný nástroj **10minutemail** (e-mail na 10 minut). [55]

Uživatel si nejprve načte webovou stránku **10minutemail.com**[10]. Pak už nemusí dělat nic, jen zkopírovat předem vygenerovaný e-mail a použít jej dle libosti. Pokud služba, do které se přihlásil vyžaduje ověření e-mailu, najde uživatel daný e-mail na 10minutemail.com pod časomírou. O tom, zda e-mail přišel informuje kolonka „Inbox“. [55]



Obrázek 7 - Výsledky nástroje 10minutemail [55]

[7] https://www.dashlane.com/
[8] https://1password.com/sign-up/?cjevent=806eb0f078f611ea813a010a0a18050f
[9] https://bitwarden.com/
[10] https://10minutemail.com/

Na druhou stranu, v případě že si uživatel přeje odeslat anonymní e-mail, a nejen vytvořit falešnou mailovou schránku, může tak učinit využitím služeb **anonymousemail.me**[11] nebo **emkei.cz**[12].

[11] https://anonymousemail.me/
[12] https://emkei.cz/

4 NÁSTROJE PRO ZACHOVÁNÍ ANONYMITY

Doposud se praktická část této práce zabývala otázkami úniků informací a aktivním sledováním uživatele ať už ze strany poskytovatele internetového připojení nebo různých společností a webových stránek.

Nyní však nastal čas se začít bránit a možná přejít i do protiútoku. V této kapitole se totiž bude práce zabývat různými nástroji, které uživateli zjednoduší cestu k anonymitě. Popíše systémová opatření, různé nastavení prohlížečů a jejich doplňky a další softwarové nástroje pro zachování anonymity uživatele.

4.1 Systémová opatření

Jedny z prvních opatření, které může uživatel při své cestě za anonymitou podstoupit, jsou právě ty systémové. Operační systémy samy o sobě nabízí mnoho užitečných nastavení, které mohou zabránit napadení počítače, únikům citlivých informací, sledování a nabourání anonymity uživatele obecně. [26]

O které nastavení a opatření jde, se pokusí práce odhalit právě v této podkapitole.

(Následující nastavení jsou cílena především na uživatele OS Windows.)

4.1.1 Aktualizace

Zatím co ve většině uživatelů mobilních zařízení vzbudí aktualizace nadšení z nově příchozích funkcí a softwarových vychytávek, uživatelům stolních počítačů a notebooků, zejména pak s operačním systémem Windows, vykouzlí taková aktualizace na tváři maximálně vrásky. Přitom se jedná o velice účinnou, přesto podceňovanou obranu proti napadnutí zvenčí. [26]

Ano, je nutné si připustit, že aktualizace s sebou většinou přináší dlouhé čekání na stáhnutí a následnou aplikaci aktualizací a také obavy, že některé věci přestanou fungovat tak jak uživatel očekává. Na druhou stranu, ale s sebou mohou přinést i záplatu na bezpečnostní rizika a díry v systému. Hackeři stále objevují nové a nové možnosti, jak proniknou do systému a uškodit uživateli, na což se Microsoft snaží okamžitě reagovat bezpečnostními aktualizacemi.

Windows 7 a 8 dělí aktualizace na „důležité“ a „volitelné“. V případě, že má uživatel počítač správně nastavený, provádí se důležité aktualizace automaticky. [26]

Pokud si uživatel svým nastavením není jistý, může si vše ověřit následovně:

- Pro Windows 7 klikne uživatel na symbol Windows v levém dolním rohu. Poté klikne na „Prohledat programy a soubory“ a napíše „Windows update/aktualizace“. Dále klikne na „Změnit nastavení“ vlevo a u kolonky „Důležité aktualizace“ zvolí možnost „Instalovat aktualizace automaticky“.
- Pro Windows 8 otevře vpravo lištu s menu a klikne na „Prohledat“. Pak si uživatel rozklikne „Nastavení“ a nahoře zadá „updates/aktualizace“. Dále pokračuje stejně jako u varianty s Windows 7, tedy „Změnit nastavení“ a „Instalovat aktualizace automaticky“. [26]

Windows 10 rozlišuje aktualizace funkcí a aktualizace pro zvýšení kvality. Krom nich rozlišuje třeba i aktualizace ovladačů nebo aktualizace definic ad. První dva zmíněné typy jsou ale nejdůležitější, jelikož s sebou nejčastěji přináší i nové zabezpečení. Windows 10 uživatele vždy upozorní o nové aktualizaci. Pokud se tomu tak nestalo nebo upozornění uživatel jednoduše přehlédl, může se o existenci nové aktualizace přesvědčit následovně:

Uživatel klikne na ikonku Windows vlevo dole a napíše „Windows update/Vyhledat aktualizace“ a možnost rozklikne. Zobrazí se mu okénko nastavení, kde si může aktualizaci vyhledat pomocí „Vyhledat aktualizace“ nebo ji přímo nainstalovat, pokud je aktualizace již nabízena, kliknutím na „Stáhnout a nainstalovat“. Dále si uživatel může aktualizace dočasně pozastavit nebo si prohlídnout historii naposledy aplikovaných aktualizací apod. [56] [57]

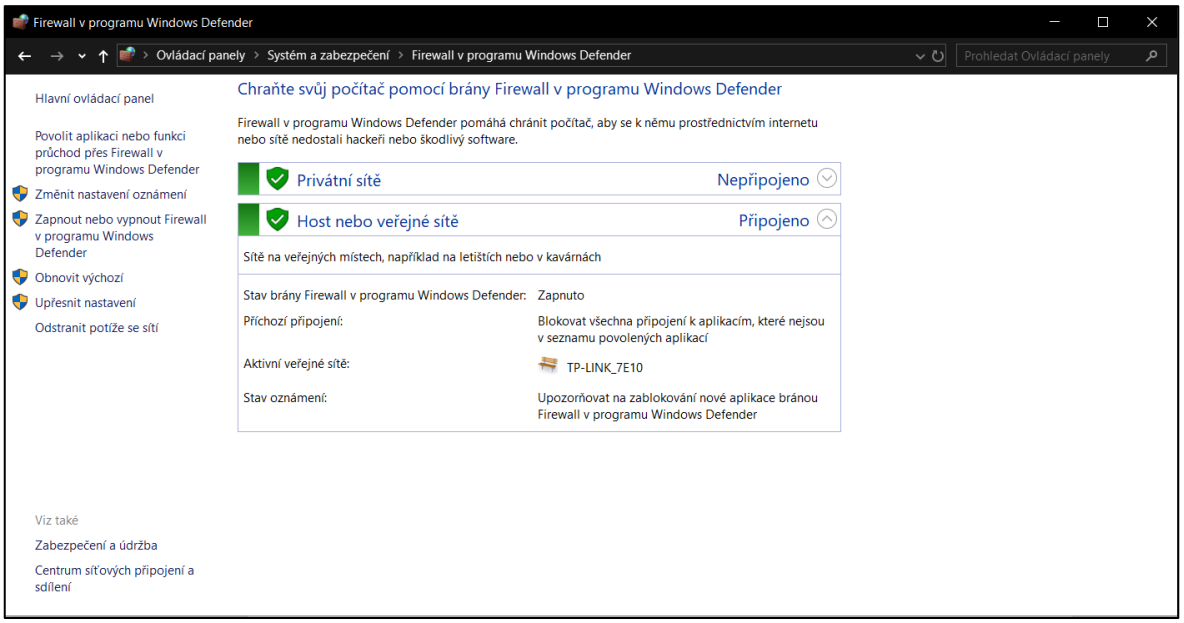
Obrázek 8 - Windows Update [57]

4.1.2 Firewall

Firewall je technické vybavení, které slouží jako brána pro komunikaci mezi sítěmi nebo mezi počítači a sítěmi a stará se, aby data putující oběma směry byla bezpečná. Firewall chrání počítač před neoprávněnými přístupy tak, že jednoduše povolí pouze komunikace, které považuje za nezbytné pro běžný provoz. Proto je důležité si v nastavení Firewallu ověřit, zda je pro danou síť zapnutý. [37]

Přístup k nastavení Windows Firewall je jednoduchý:

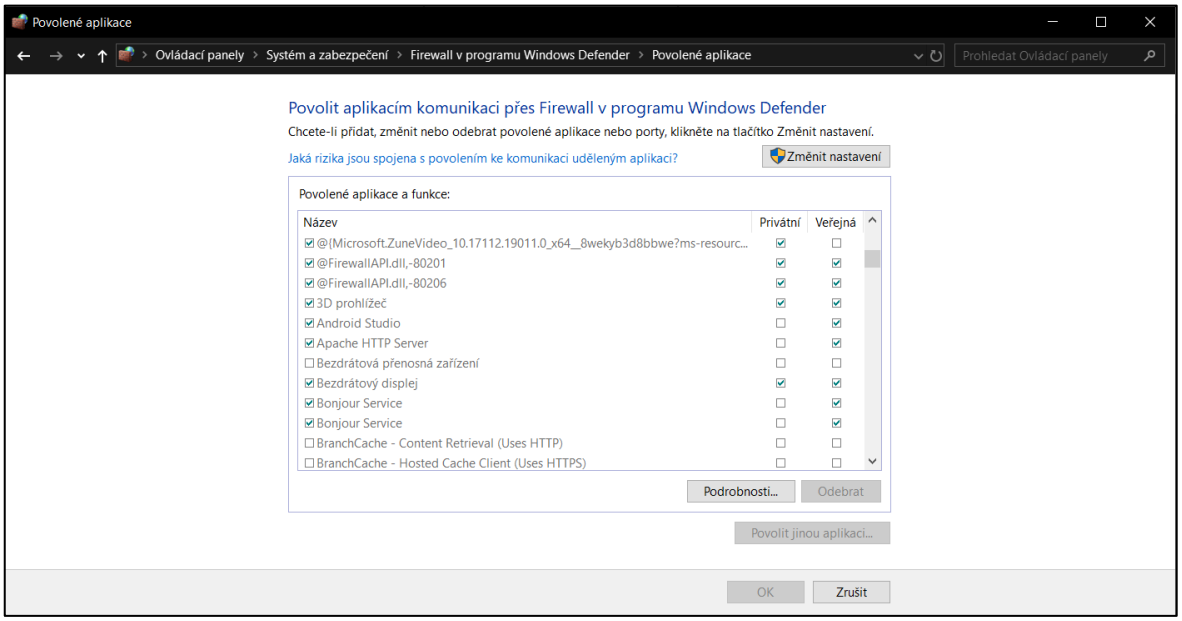
- V operačních systémech Windows 7 a 8 uživatel klikne na ikonku Windows, zvolí „Ovládací panely“ a poté „Brána Windows Firewall“. [26]
- V operačním systému Windows 10 uživatel kline na ikonku Windows vlevo dole, do vyhledávání napíše „Ovládací panely“ a rozklikne je. Dále zvolí „Systém a zabezpečení“ a pak rozklikne „Firewall v programu Windows Defender“.



Obrázek 9 - Firewall v programu Windows Defender [26]

Windows rozlišuje soukromé a veřejné sítě. Soukromé sítě Windows chápe jako domácí či pracovní sítě a bere je více méně jako bezpečné. Naopak veřejné sítě vnímá poněkud skeptičtěji. Předpokládá, že veřejná síť není bezpečná, proto na ni aplikuje příslušná bezpečnostní pravidla. To ovšem může někdy působit různé systémové chyby nebo pády jednotlivých aplikací. [26]

Chování Windows vůči jednotlivým aplikacím z hlediska Firewallu může být ovlivněno v dalším nastavení. Stačí kliknout na „Povolit aplikaci nebo funkci průchod přes Firewall v programu Windows Defender“. [26] [37]



Obrázek 10 – Povolení přístupu přes Firewall [26]

V tomto nastavení si uživatel může zvolit, které aplikace a funkce budou moct komunikovat skrze bránu Firewall. [37]

Dobrou alternativu pro Windows Firewall nabízí například Norton 360 Deluxe, Bitdefender Total Security nebo Avast Premium Security. Co se týče bezplatných alternativ, za zmínku stojí SolarWinds Network Firewall Security Management, ZoneAlarm nebo Comodo Firewall. [58] [59]

4.1.3 Windows Defender

Užitečným nástrojem OS Windows je Windows Defender. Ten byl původně konstruován jako program chránící citlivé informace uživatele před spyware. Postupem času se z něj ale vyklubala i velice schopná antivirová ochrana. [26]

Nejedná se sice o nejšpičkovější software v tomto oboru, ale je schopen ochránit uživatele od většiny nejčastějších a nejrizikovějších hrozeb. Windows Defender pokulhává spíš v oblasti ochrany uživatele před otravným adwarem a podobnými riziky. To ale pro čtenáře nemusí být nezbytně problematické, jelikož tímto okruhem hrozeb se práce zabývá v další kapitole.

Pokud se tedy uživatel kromě nabourání jeho anonymity obává i škodlivých virů a podobných nebezpečí, ale nechce ztrácet čas hledáním a instalací jiných antivirových programů, je pro něj vložení bezpečnosti do rukou Windows Defender optimálním řešením. [60]

4.2 Nastavení prohlížeče a užitečné doplňky

Klíčovým nástrojem pro pohodlný přístup na Internet je prohlížeč. Těch je v dnešní době velká spousta a většina z nich toho může při nevhodném nastavení o uživateli mnoho říct. Popisováním nastavení každého jednoho prohlížeče by zabralo zbytečně moc času, a protože se často moc neliší, zaměří se práce pouze na jeden, a to prohlížeč Google Chrome. [61]

4.2.1 Vyčištění počítače

Google Chrome disponuje funkcí „Vyčištění počítače“, která uživateli pomůže najít v počítači podezřelé či nežádoucí programy. Pokud takové programy chrome odhalí, zobrazí jejich seznam uživateli, a ten je může jednotlivě vymazat kliknutím na tlačítko „Odstranit“. Tato funkce je přístupná v rozšířeném nastavení Google Chrome. [61]

Uživatel si nejprve spustí Google Chrome. Dále otevře možnosti (symbol tří teček pod tlačítkem „zavřít“ vpravo nahoře) a zvolí „Nastavení“. Dole pak klikne na „Rozšířená nastavení“ a dále na „Vyčištění počítače“. Nakonec uživatel zvolí „Najít“ a počká si na výsledek analýzy. [61]

4.2.2 Ochrana soukromí a zabezpečení

V nastavení v kolonce „Ochrana soukromí a zabezpečení“ se nachází šikovné nástroje chránící soukromí uživatele.

Po kliknutí na možnost „Nastavení webu“ se uživateli zobrazí nastavení, které může omezit jaký obsah mohou stránky zobrazovat a s jakými daty mohou pracovat při jejich prohlížení.

Zde uživatel najde mezi jinými i nastavení souborů cookies, polohy, kamery a mikrofonu, JavaScriptu, Flash obsahu atd. Většina výchozích nastavení je vyhovujících. Uživatel si zde, ale může nastavení změnit dle libost.

Například v nastavení „Soubory cookie a data webových stránek“ může uživatel úplně zakázat cookies nebo třeba nastavit jejich vymazání po vypnutí prohlížeče. Doporučeným

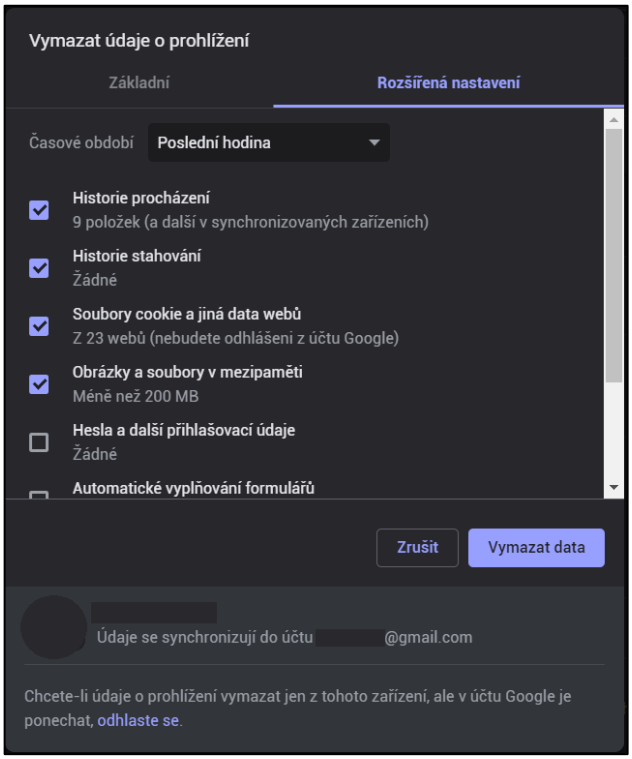
nastavením je možnost „Blokovat soubory cookie třetích stran“. Uživatel by ale měl mít na mysli, že tato nastavení mohou ovlivnit správný chod webových stránek a aplikací. [37]

Další nastavení týkající se soukromí může uživatel nalézt v kolonce „Ochrana soukromí a zabezpečení“ po kliknutí na možnost „Více“. [37]

4.2.3 Mazání údajů o prohlížení

Kolonka „Ochrana soukromí a zabezpečení“ v nastavení Google Chrome obsahuje i další užitečný nástroj, a to možnost „Vymazat údaje o prohlížení“.

Tato možnost se netýká jen historie prohlížení, historie stahování, ale také souborů cookies, obrázků v mezipaměti, hesel a přihlašovacích údajů ad. [37] [62]



Obrázek 11 - Vymazat údaje o prohlížení [37] [62]

Pokud by si uživatel přál smazat pouze jen některé konkrétní položky z historie prohlížení, může tak udělat v Historii Chromu. Přístup do Historie Chromu je jednoduchý. Uživateli se zobrazí po stlačení kláves Ctrl + H. [62]

4.2.4 Anonymní režim

Pokud si uživatel nepřeje ukládat historii, údaje z formulářů nebo soubory cookies, může použít tzv. „Anonymní režim“. Je nutno ale podotknout, že uživatel může být nadále

sledován navštívenými weby nebo poskytovatelem internetového připojení ad. Název „Anonymní režim“ tedy do určité míry ztrácí svůj smysl. Své opodstatnění najde například u sdíleného PC, kdy si jeden uživatel nepřeje, aby byla jeho aktivita na Internetu viditelná dalšími uživateli. [63]

Anonymní režim nabízí většina prohlížečů. U Google Chrome může uživatel do tohoto režimu vstoupit stiskem kláves Ctrl + N. Na nově zobrazeném anonymním okně se nejdříve zobrazí popis nástroje a výše zmíněné podmínky. [63]

Obrázek 12 - Anonymní režim [63]

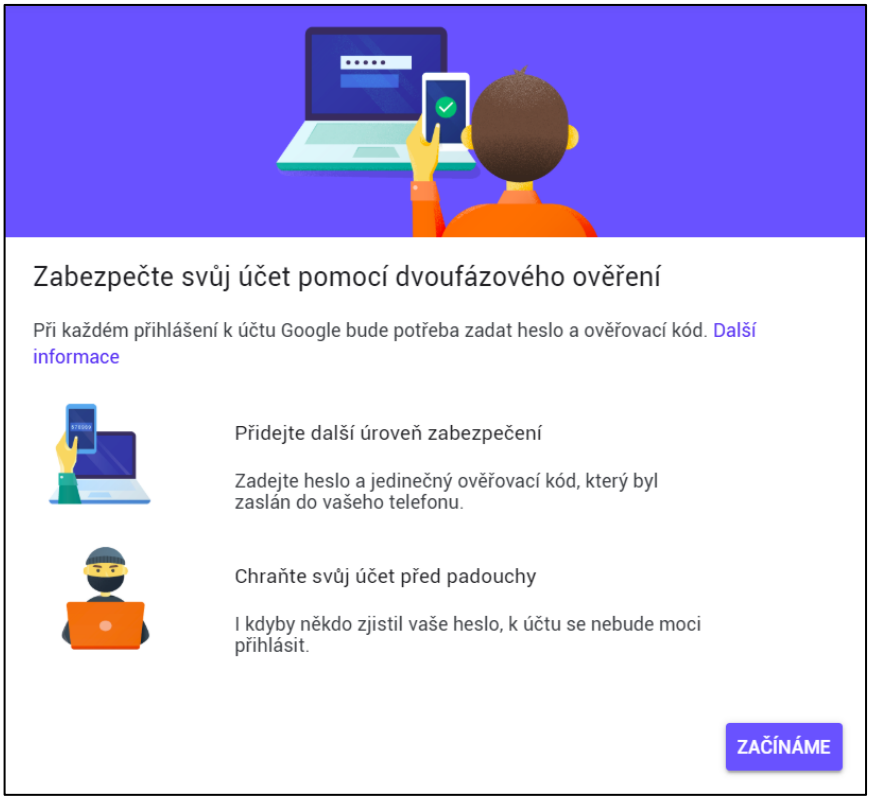
4.2.5 Personalizace reklam

Pro omezení sběru dat o vašem Google účtu za účelem cílené reklamy je dobré vypnout personalizaci reklam. Tuto možnost uživatel najde ve správě svého Google účtu. Jednoduše klikne na uživatelskou ikonku vpravo nahoře a zvolí „Spravovat váš účet Google“. Dále rozklikne kolonku „Data a personalizace“ v levém menu a najde si okénko „Personalizace reklam“. Personalizaci reklam pak může vypnout v nastavení reklam po zvolení „Přejít do nastavení reklam“. [64]

4.2.6 Dvoufaktorová autentizace

Google Chrome svým uživatelům nabízí vlastní implementaci dvoufaktorové autentizace. Jde o technologii, která pro přístup k účtu kromě hesla vyžaduje i jiný druh ověření. Dá se tím tak zabránit ukradení identity v případě ztráty důvěryhodnosti hesla. Tato možnost je přístupná ve správě Google účtu.

Uživatel nejdříve klikne na uživatelskou ikonku vpravo nahoře a zvolí „Spravovat váš účet Google“. V levém menu si zvolí „Zabezpečení“ a v kolonce „Přihlášení do Googlu“ si vybere „Dvoufázové ověření“. Poté už uživatele jednotlivými kroky aktivace dvoufázového ověření přehledně provede Google. [65]



Obrázek 13 - Dvoufázová autentizace [65]

4.2.7 Adblock Plus

Jedním z důvodů, proč byl k demonstraci různých prohlížečových opatření pro anonymitu a soukromí vybrán právě Google Chrome je internetový obchod chrome[13], který nabízí širokou škálu prohlížečových doplňků zdarma, přičemž je jejich aplikace naprosto

[13] https://chrome.google.com/webstore/category/extensions?hl=cs

jednoduchá. Zde lze také najít mnoho výborných nástrojů pro blokování reklam. Jedním takovým je Adblock Plus.

Po načtení stránky internetového obchodu chrome, zadá uživatel do vyhledávání „Adblock plus“ nebo „Adblock“. Vyskočí nabídka různých nástrojů naplňujících podobný účel. Uživatel si o nástrojích může přečíst více jednoduše klepnutím na položku nebo ho přímo aplikovat kliknutím na tlačítko „Přidat do Chromu“. [66]

Obrázek 14 - Adblock Plus [66]

Adblock Plus schopně blokuje otravné reklamy, video reklamy, bannery, vyskakovací okna a podobně a je celosvětově využíván mezi milióny uživatelů. Verze tohoto nástroj je přístupná i ostatním prohlížečům na **getadblock.com**[14]. [67]

4.2.8 Privacy Badger

Privacy Badger, podobně jako Adblock Plus, umí blokovat otravné reklamy. Kromě toho také zvládá blokování trackerů třetích stran, které by mohly uživatele sledovat, a to všechno samostatně, bez potřeby hlubších znalostí či otravného nastavování. Učí se totiž automaticky sám, kdy detekuje sledovací prvky během toho, co uživatel pracuje s Internetem.

Privacy Badger je dostupný na stránkách **privacybadger.com**[15] nebo v internetovém obchodě chrome. Pro aplikaci nástroje stačí kliknout na „Přidat do Chromu“ stejně jako v případě Adblocku. [68]

4.2.9 Disconnect

Disconnect patří mezi další nástroje, které se starají o soukromí a anonymitu uživatele. Podobně jako Privacy Badger blokují trackery třetích stran a stovky neviditelných trackerů

[14] https://getadblock.com/
[15] https://privacybadger.org/

denně. To nejen chrání anonymitu uživatele, ale podle Disconnect i zvyšuje rychlost načítání webových stránek a aplikací až o 44 %.

Disconnect je zdarma k mání na **disconnect.me**[16] nebo v internetovém obchodě chrome. [69]

4.2.10 Ghostery

Na rozdíl od Disconnect nebo Privacy Badger volí Ghostery méně radikální přístup v oblasti blokování obsahu stránek. Prvky pro uživatele neškodné nechává projít svým filtrem, a tak se méně často stává, že by stránky přestaly fungovat tak, jak mají. Navíc Ghostery poskytuje uživateli detailnější nastavení než předchozí nástroje, což některým může vyhovovat více, některým méně. Rozšířená verze Ghostery Midnight ještě navíc poskytuje další technologie, jako například zabudovanou VPN. Tato verze je však už měsíčně zpoplatněna.

Ghostery je dostupný na **ghostery.com**[17] nebo v internetovém obchodě chrome. [70]

4.2.11 HTTPS Everywhere

Jedná se o prohlížečový doplněk, který se snaží automaticky používat na všech stránkách šifrovaný protokol HTTPS místo nezabezpečené komunikace přes HTTP.

Balíček je dostupný na internetovém obchodu chrome nebo na stránkách **eff.org/https-everywhere**[18]. [71]

4.2.12 NoScript

NoScript chrání uživatele před škodlivými scripty a sledováním trackery třetích stran. Funguje tak, že ve svém výchozím nastavení zakáže na každé stránce všechny scripty. Uživatel si pak může sám vybrat, které scripty na stránce povolí v nastavení toho nástroje. Většinou však dochází k narušení správného fungování webové stránky či aplikace a uživatel jen nucen povolit alespoň scripty vázané konkrétně na tuto stránku, aplikaci.

Toto prohlížečové rozšíření je dostupné na **noscript.net**[19] nebo na internetovém obchodě chrome. [72]

[16] https://disconnect.me/
[17] https://www.ghostery.com/?utm_source=ghostery.com&utm_campaign=install_ghostery_hp
[18] https://www.eff.org/https-everywhere
[19] https://noscript.net/

4.2.13 AdNauseam

Nyní nastává čas protiútoku. Skrývání se a blokování reklam či snaha vyhnout se sledování je jednou účinnou metodou, ale existují další vynalézavé cesty, jak zmást nepřítele. Jedním z těchto nástrojů je právě AdNauseam.

„Klikám na reklamy, abyste vy nemuseli“, to je motto AdNauseam. Jedná se o prohlížečové rozšíření, které na jedné straně chrání uživatele před otravnými reklamami a na straně druhé bojuje proti společnostem, které neberou ohled na soukromí uživatele. Tento doplněk totiž využívá zmatek ke zmatení nepřítele. Tajně kliká na všechny dostupné reklamy, viditelné či neviditelné a zahlcuje tak jejich majitele irelevantními daty.

AdNauseam je dostupný na **adnauseam.io**[20].

Instalace je poněkud složitější, protože toto rozšíření Google stáhl ze svého internetového obchodu chrome.

1. Nejdříve si uživatel musí otevřít web zmíněný výše a kliknout na fialové tlačítko „Install AdNauseam“ vpravo nahoře.
2. Bude přesměrován na Github, kde je popis instalace.
3. Pak si musí stáhnout poslední verzi tohoto rozšíření, kterou najde po kliknutí na odkaz „releases page“[21]. To následně extrahovat někam, kde nebude zavázet (nejlépe třeba do Program Files).
4. Uživatel si v prohlížeči otevře nastavení rozšíření. Pokud si není jistý navigací přes nastavení, stačí do odkazového řádku zadat: chrome://extensions/.
5. Uživatel si následně zapne „Režim pro vývojáře“ vpravo nahoře a klikne na „Načíst nerozbalené“ v levém horním rohu.
6. Pak otevře extrahovanou složku, čímž by měla být instalace hotová. (Uživatel by měl pamatovat, že by měl otevřít složku „adnauseam.chromium“ bez čísla verze, která je v extrahované složce, ne extrahovanou složku samotnou.)
7. Po instalaci je uživatel přesměrován do nastavení AdNauseam, kde si může zvolit, které služby AdNauseam bude chtít využívat. [73]

[20] https://adnauseam.io/
[21] https://github.com/dhowe/AdNauseam/releases/tag/v3.9.104

4.2.14 TrackMeNot

TrackMeNot má podobný přístup jako AdNauseam. Pomáhá uživateli od sledování a profilování dat pomocí chaosu.

TrackMeNot je v podstatě proces s nízkou prioritou běžící na pozadí, který v pravidelných intervalech vydává náhodné vyhledávací dotazy. Tím účinně zásobuje reklamní společnosti a webové stránky falešnými a irelevantními informacemi, mezi kterými se opravdové údaje o uživateli jednoduše ztratí.

TrackMeNot je dostupný na **trackmenot.io**[22] nebo na internetovém obchodě chrome. [74]

4.2.15 Windscribe

Windscribe je VPN/proxy prohlížečové rozšíření a VPN počítačová aplikace, která kromě skrývání IP adresy a virtuální privátní sítě nabízí i šifrování aktivity prohlížení, vlastní řešení firewall pro ochranu osobních dat v momentě přerušení spojení s VPN, blokování trackerů a reklam a spoustu dalších nástrojů.

Po potvrzení ověřovacího e-mailu po registraci, je uživateli přiděleno 10 GB měsíčního surfování na Internetu pod VPN zdarma. Uživatel se vždy může rozhodnout pro rozšíření na plnou verzi, která je sice zpoplatněná, ale nepřináší s sebou žádné datové omezení.

Windscribe je dostupný na **windscribe.com**[23] nebo v internetovém obchodě chrome. [75]

Obrázek 15 - Windscribe browserová aplikace [75]

[22] https://trackmenot.io/
[23] https://windscribe.com/

4.3 Nástroje pro anonymizaci

Na konci předchozí podkapitoly práce lehce nakousla nástroje anonymizace jako VPN a proxy servery. Těmito a dalšími nástroji, jako například anonymní prohlížeč tor nebo systém kodachi, se bude práce více zabývat v této závěrečné podkapitole.

4.3.1 Proxy server ve Windows 10

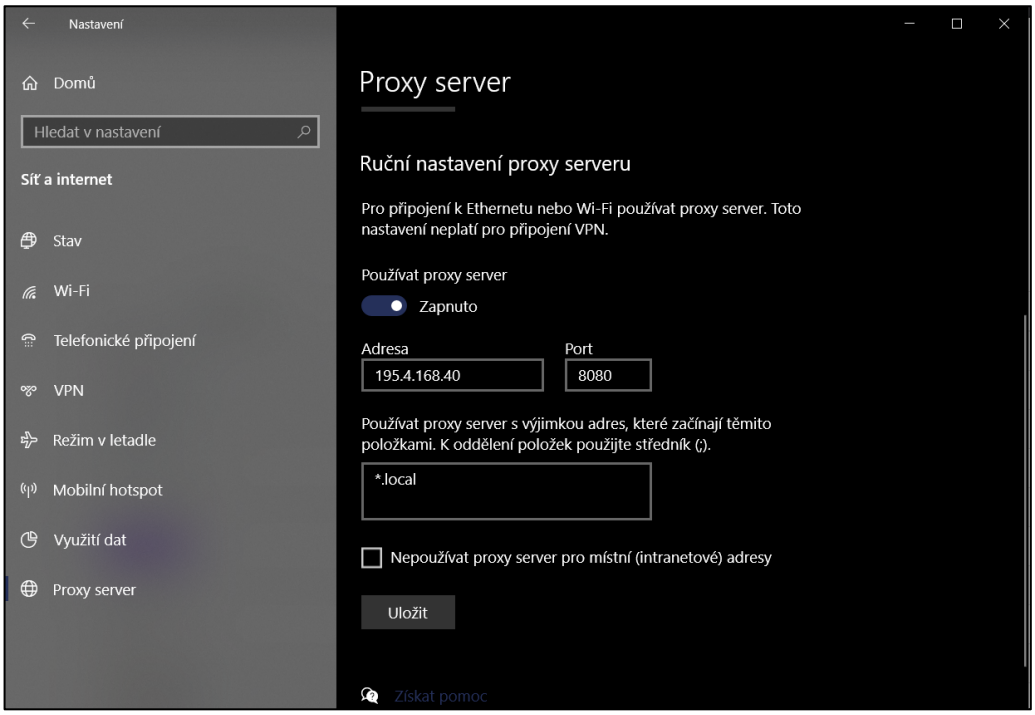
Jednou z možností, jak může uživatel skrýt svou reálnou IP adresu jsou proxy servery.

Při stisknutí klávesové zkratky Windows + I se uživateli zobrazí nastavení Windows. Zde uživatel klikne na „Síť a Internet“ a v levém menu zvolí možnost „Proxy server“. Dole v kolonce „Používat proxy server“ přepne na „Zapnuto“ a vyplní adresu a port proxy serveru. Nakonec uživatel klikne na uložit.

Zda proxy server funguje si uživatel může ověřit na **whatismyip.com**[24].

Seznam proxy serverů zdarma může uživatel najít například na **free-proxy-list.net**[25].

Dále by bylo také dobré zmínit, že proxy servery zdarma mohou být nezabezpečené a často pomalé. Lepší alternativou jsou proto služby VPN, které jsou popsány níže. [76]



Obrázek 16 - Nastavení proxy serveru ve Windows 10 [76]

[24] https://www.whatismyip.com/
[25] https://free-proxy-list.net/

4.3.2 VPN služba ve Windows 10

Síť VPN umožňuje uživateli bezpečně a anonymně surfovat po Internetu a také obcházet geografické blokování různých služeb. Jde o komunikaci s Internetem přes vzdálený server, k němuž je uživatel připojen pomocí bezpečné virtuální privátní sítě.

Nicméně mnoho VPN služeb je placených a jejich bezplatné verze jsou buď omezené na rychlosti nebo na objemu přenesených dat. Na druhou stranu je dobré mít na paměti, že hodně VPN služeb nabízených zdarma jsou méně kvalitní nebo samy porušují soukromí uživatele sběrem dat o jeho aktivitě. [77]

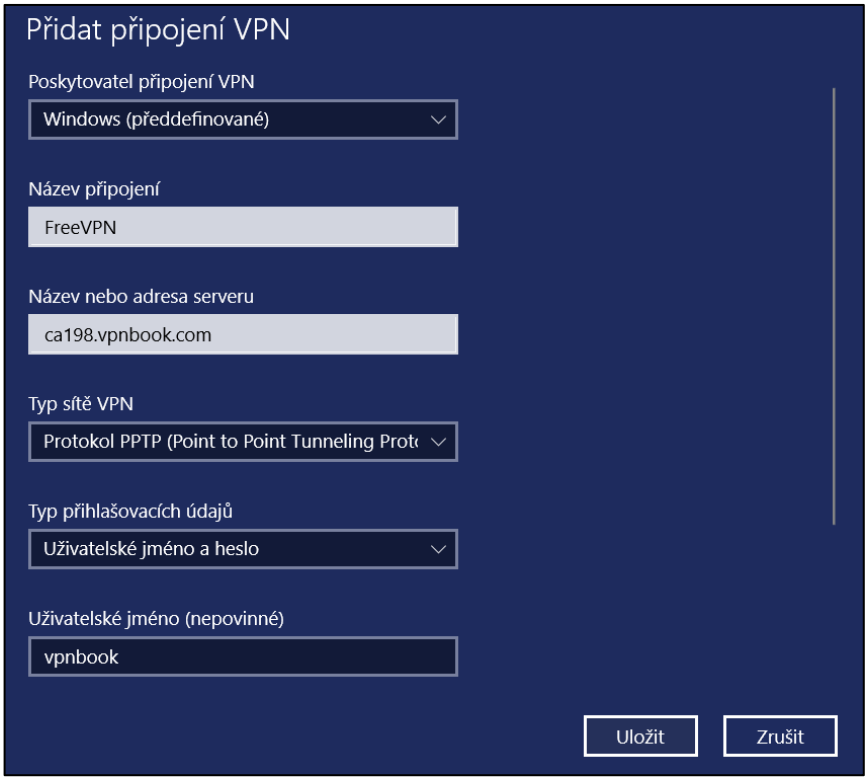
Na stránce **vpnbook.com**[26] najde uživatel v sekci „free VPN“ v levém sloupečku konfiguraci Free PPTP VPN. Výhodou této možnosti je, že si uživatel nemusí nic stahovat a VPN si pohodlně nastavit v prostředí svého operačního systému zdarma.

Uživatel nejprve stiskne klávesovou zkratku Windows + I, načež se otevře nastavení Windows. Pak přejde do nabídky „Síť a Internet“ a v levém menu zvolí možnost „VPN“. Dále klikne na tlačítko „Přidat připojení VPN“. V nově otevřeném okně si v kolonce „Poskytovatel připojení VPN“ zvolí možnost „Windows (předdefinované)“. V kolonce „Název připojení“ pak uvede libovolný název. Jako „Název nebo adresa serveru“ uživatel zadá adresu, kterou si vybral na výše zmíněném webu (viz obrázek 17). Jako „Sítě VPN“ zvolí „Protokol PPTP (Point to Point Tunneling Protocol)“. Nakonec si za typ přihlašovacích údajů vybere „Uživatelské jméno a heslo“ a kolonky „Uživatelské jméno“ a „Heslo“ vyplní dle údajů na dříve zmíněném webu. [77]

Po úspěšné konfiguraci VPN už stačí kliknout na „Připojit“.

Pokud by došlo k chybám může uživateli pomoct vymazání a nová instalace síťových adapterů ve správci zařízení, aktualizace Windows a restartování nebo povolení protokolu PPTP v bráně firewall. [77]

[26] https://www.vpnbook.com/freevpn



Obrázek 17 - PPTP VPN nastavení [77]

Další možností je využít klienta OpenVPN, jehož instalací a nastavením uživatele provede šikovný tutoriál v sekci „How-To“ na stránkách **vpnbook.com**[27].

Stránka vpnbook.com také umožňuje anonymní vyhledávání přes proxy server (viz obrázek 18). Stačí kliknout na záložku „Free Web“ a použít nabízený vyhledávač.

Obrázek 18 - Vyhledávání přes proxy [77]

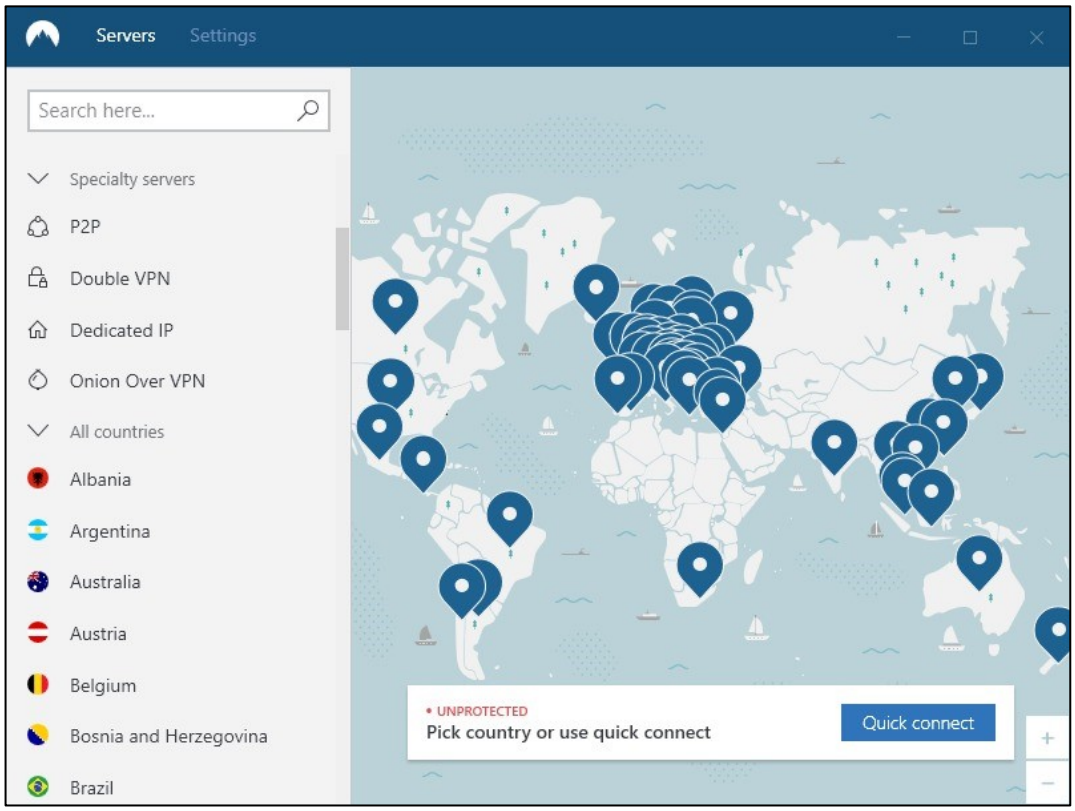
[27] https://www.vpnbook.com/howto/setup-openvpn-on-windows10

4.3.3 NordVPN

NordVPN je placená služba VPN s nejširší sítí VPN serverů na světě. Tato síť čítá přibližně 5700 VPN serverů v 59 zemích. Mimo to nabízí vysokou rychlost připojení, se kterou se spousta neplacených i placených VPN nemůže srovnávat. S faktory jako silné 256 bitové šifrování, kvalitní VPN protokoly a hezké, čitelné rozhraní hravě dostála svého titulu „Nejlepší VPN roku 2020“. [78]

Předplatné je trošičku dražší než u ostatních služeb, ale při dlouhodobějších předplatných a pravidelných slevách je už cena přívětivější. Po uhrazení předplatného je software okamžitě k mání a uživatel si jej může stáhnout a nainstalovat.

NordVPN je dostupná na **nordvpn.com**[28]. [78] [79]



Obrázek 19 – NordVPN [78]

V přehledném nastavení se uživatel určitě neztratí. V levé nabídce si může vybrat buď ze speciálních serverů jako peer-to-peer servery, připojení přes dvě VPN apod. nebo si vybrat konkrétní zemi pro připojení k VPN serveru. Nahoře si pak může zvolit záložku „Settings“,

[28] https://nordvpn.com/

kde najde různé užitečné nástroje, jako nastavení vlastní adresy DNS nebo aktivace speciálních maskovaných serverů. [78] [79]

4.3.4 PureVPN

Jedna z nejvýhodnějších alternativ ve světě VPN v kategorii cena/výkon je momentálně PureVPN. Ta nabízí více než 2000 serverů v přibližně 140 zemích, šifrování a základní bezpečnostní opatření. Ke všemu nabízí i více než slušnou rychlost přenosu dat, která je schopná zvládnout i streamování. [80]

PureVPN je dostupný na **purevpn.com**[29].

4.3.5 Tor

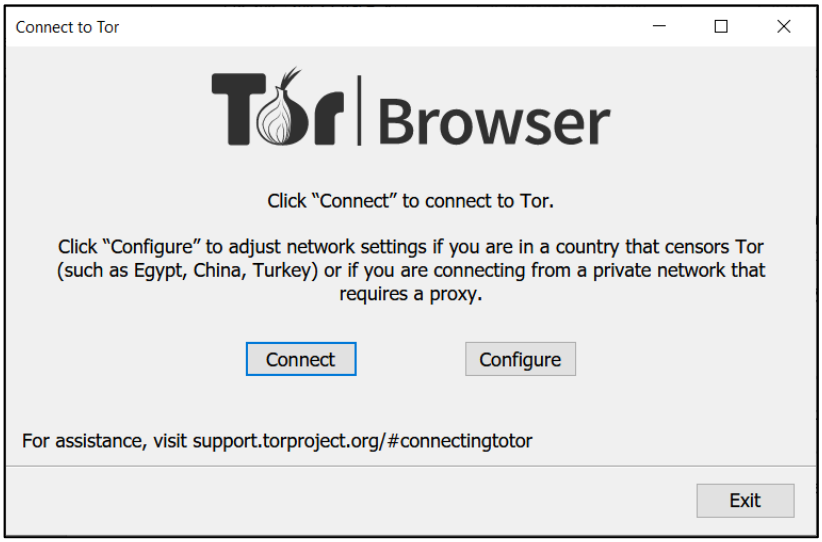
Tor je speciální anonymizační síť, která pro svůj chod využívá tzv. onion routing. Jde techniku anonymní komunikace, kdy jsou data šifrována a jejich přenos je realizován přes několik počítačů, které může uživatel chápat jako vrstvy. Dalo by se tomu rozumět i jako více proxy serverů zapojených za sebou, kde konkrétní informace mají vždy jen dva po sobě jdoucí servery. Ke všemu je síť kromě šifrování opatřena i šumem, tvořeným proudy packetů, které vytváří chaos a znesnadňují tak odposlech. Tato síť by se díky svému vrstvení dala přirovnat k cibuli, proto onion routing. [36] [37]

Na webových stránkách **torproject.org**[30] si uživatel může stáhnout speciální prohlížeč, který využívá onion routingu. Nabídka ke stažení se uživateli zobrazí hned po otevření těchto webovek na jejich úvodní stránce. Po kliknutí na „Download Tor Browser“ si ještě uživatel bude moci vybrat verzi pro příslušný operační systém a zahájí se stahování. Následuje jednoduchá instalace. [81]

Při prvním nastartování prohlížeče Tor je uživateli nabídnuta možnost konfigurace prohlížeče nebo přímé připojení do sítě Tor. V případě, že uživatel využívá například nějakého proxy serveru nebo se nachází ve státě, kde je služba Tor cenzurovaná je vhodné, aby si zvolil možnost „Configure“. Tor v České republice žádné cenzuře nepropadá, ale uživatele by mohlo zajímat nastavení spojené s připojením k Internetu přes proxy server. V případě, že proxy server používá, jednoduše zadá příslušné informace do formuláře

[29] https://www.purevpn.com/why-purevpn
[30] https://www.torproject.org/

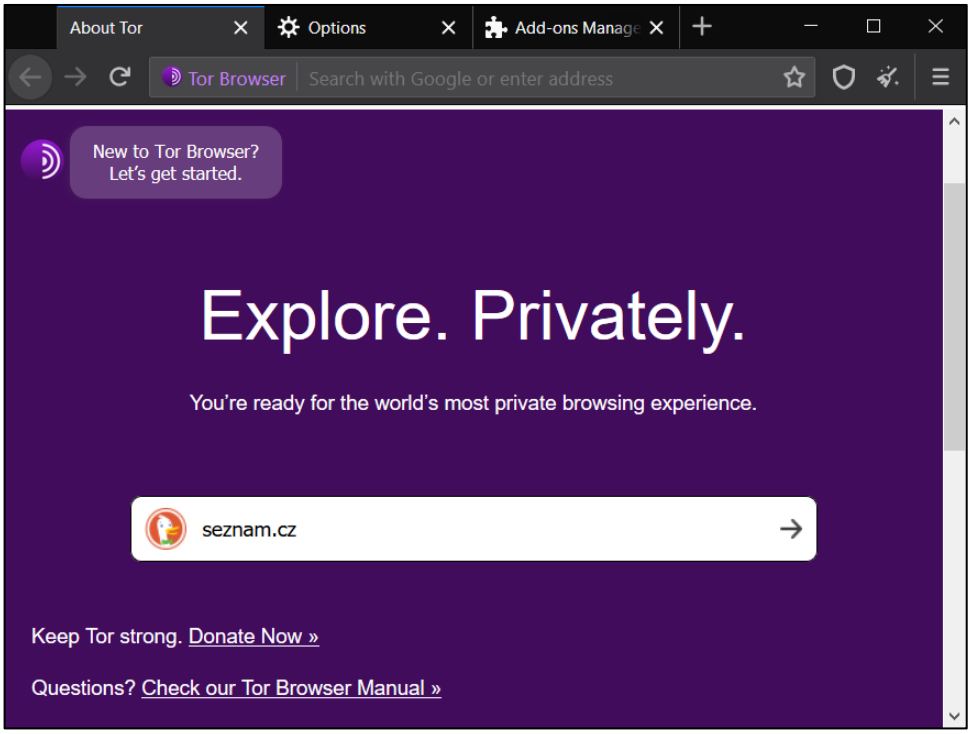
v nastavení zobrazeném na obrázku níže. Jinak může uživatel s čistým svědomím kliknout na tlačítko „Connect“ a do pár sekund se objeví v prostředí prohlížeče Tor. [82]



Obrázek 20 - Tor první spuštění [81]

Obrázek 21 - Tor konfigurace [81]

Vyhledávač Tor používá jako výchozí vyhledávací engine DuckDuckGo. Uživatel si ho ale může podle libosti změnit třeba na Google v nastavení, kde najde i mnoho dalších možností modifikace prohlížeče podobných jako u ostatních prohlížečů. Stejně jako u nich ani zde nechybí správa balíčků a rozšíření, takže si uživatel může doinstalovat další nástroje pro anonymitu, jako třeba ty zmíněné v předchozí podkapitole. [81]



Obrázek 22 - Tor úvod [81]

4.3.6 Brave

Brave je další alternativou bezpečného vyhledávače. Sice nedisponuje takovou úrovní anonymity jako Tor, ale i přesto zdatně blokuje reklamy a brání trackerům ve sledování uživatele. Kromě toho přichází s novým přístupem, kdy uživateli dává možnost si vybrat, zda chce sledovat určité reklamy, za což je následně odměněn. Brave nabízí i vyšší rychlost a menší spotřebu baterie. [83]

Zatímco u většiny prohlížečů, jako například Google Chrome, je anonymní režim dobrý leda k tomu, že nezanechává historii prohlížení, anonymní režim vyhledávače Brave bere soukromí svých uživatelů mnohem vážněji. Brave má dva anonymní režimy. Běžný anonymní režim, do nějž se uživatel může dostat klávesovou zkratkou „Ctrl + Shift + N“ a anonymní s onion routingem, který používá k vyhledávání technologii Tor. Do tohoto režimu vstoupí uživatel klávesovou zkratkou „Alt + Shift + N“. [83]

Ke všemu ještě Brave nabízí skvělý design a intuitivní přístup. Pokud uživatel přemýšlí, že by opustil svůj stávající prohlížeč, ale nechce se mu znovu všechno nastavovat, nemusí se dále rozhodovat. Brave velmi rychle a plynule přesune nejen záložky, ale i doplňky a

rozšíření původního prohlížeče, včetně hesel a dosavadní historie prohlížení, takže se uživatel okamžitě cítí jako doma. [83]

Brave je dostupný na **brave.com**[31]. [83]

4.3.7 Kodachi

Posledním nástrojem pro anonymizaci uživatele, který bude v této práci popsán je Kodachi. Kodachi je Linuxový operační systém založený na Xubuntu 18.04. Jde o zabezpečený proti forenzní a anonymní operační systém, poskytující všechny možné nástroje, které by mohl uživatel pečující o své soukromí potřebovat. [84]

Kodachi běží kompletně z paměti RAM, tudíž po sobě fyzicky nezanechává žádné stopy. O to se navíc stará i technologie RAM wiping při restartu počítače. Kromě toho je veškerá komunikace po síti vynuceně realizována přes šifrovanou Kodachi VPN případně jinou VPN. DNS je zde řešeno buď přímo pomocí Tor DNS nebo DNScryptem na předdefinovaný seznam DNS serverů, které podporuji šifrované překládání doménových jmen na IP adresy. [85]

Uživatel zde nalezne hned několik bezpečných prohlížečů, mezi nimiž je například Tor nebo Firefox. Nejlepší možností je ale používat prohlížeč Kodachi, který byl sestaven autory systému Kodachi a proto má v tomto prostředí i největší podporu co se týče anonymizačních nástrojů. Je také správně přednastaven, proto si uživatel se svým soukromím při vyhledávání nemusí dvakrát lámat hlavu. [84]

V systému nechybí ani běžné aplikace jako kalendář, VLC či LibreOffice. [85]

Operační systém Linux Kodachi je dostupný na **digi77.com**[32]. Zde uživatel najde také i stručný popis systému se všemi funkcemi a dalšími informacemi, jako například postup instalace a použití, různé užitečné odkazy nebo přihlašovací údaje do systému apod.

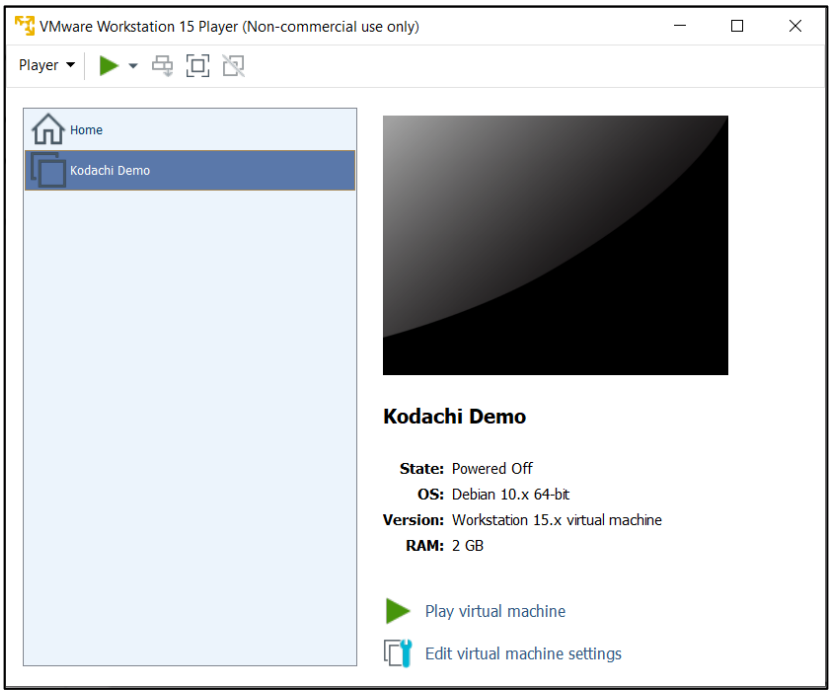
Uživatel si může vybrat mezi třemi způsoby použití Kodachi. Může tento systém spusti ve virtuálním prostředí jako je například **VMware Workstation Player**[33] nebo **Oracle VM VirtualBox**[34], přičemž autor doporučuje spíše VMware, který je rychlejší. Další možností, jak Kodachi používat je bootování z DVD nebo USB Flash paměti, na kterou uživatel systém

[31] https://brave.com/
[32] https://www.digi77.com/linux-kodachi/
[33] https://my.vmware.com/web/vmware/free#desktop_end_user_computing/vmware_workstation_player/15_0
[34] https://www.virtualbox.org/wiki/Downloads

vypálí například pomocí technologií **UniversalnUSB Installer**[35] nebo Etcher, Rufus, YUMI či v případě DVD DAEMON tools. Poslední možností je pak stáhnout si ISO soubor Kodachi, vypálit jej třeba na DVD či USB Flash disk a nainstalovat jej jako svůj primární operační systém. [84] [85]

Pro účely této práce autor zvolil možnost spustit operační systém Kodachi jako virtuální počítač přes VMWare. Po instalaci VMware si jej uživatel otevře a zvolí „Create a New Virtual Machine“. Pak zvolí cestu k souboru ISO se systémem Kodachi. Dále zvolí možnost „Linux“ a jeho distribuci, nejlépe Debian 10.x verze 64-bit. Nakonec může zvolit parametry systému.

Po dokončení tvorby virtuálního počítače ho stačí jen zvolit a kliknout na „Play virtuál machine“ a systém se nabootuje. [84]



Obrázek 23 - Vytvoření virtuálního stroje s Kodachi [84]

Po nabootování uživatele přivítá systém Kodachi. V pravém rohu lze nalézt různé užitečné parametry jako VPN, IP adresa, ping, poloha, MAC adresa atd. a upozorňují uživatele o jejich stavu v reálném čase, takže si je uživatel nemusí sám dohledávat. V dolním baru zase

[35] https://www.pendrivelinux.com/universal-usb-installer-easy-as-1-2-3/

na uživatele čekají nastavení týkající se DNS serverů, VPN nebo prohlížeče. Na levé straně je pak lišta, která skrývá zejména systémová nastavení a další. [84]

Obrázek 24 - Operační systém Kodachi [84]

Kodachi poskytuje širokou škálu nástrojů a metod jak za sebou na Internetu zamést stopy. Je to skvělá volba pro pokročilé uživatele, kteří se zajímají o svoje soukromí a anonymitu. [85]

ZÁVĚR

Tato bakalářská práce v teoretické části seznámila čtenáře s historií, vývojem a možnou budoucností Internetu a představila mu anonymitu jak z informačního a teoretického hlediska, tak z hlediska jejího etického aspektu. Práce představila čtenáři myšlenku, anonymity jako opravdové svobody na Internetu a jaký vliv na ni mají rozhodnutí jednotlivců.

V praktické části práce nejprve poodhalila způsoby sledování, které využívají společnosti a webové stránky. Dále zbořila mylné představy o anonymních režimech apod. Práce představila čtenáři technologie jako cookies, IP adresy a sledování polohy, skripty a fingerprinting. Kromě toho i ukázala jakým způsobem zjistit, zda je uživatel dostatečně bráněný proti těmto metodám a zda ho lze či nelze sledovat.

Čtenář se dále mohl dočíst i něco o únicích informací a o způsobu, jak zjistit, zda jeho data nebyla kompromitována. Kromě toho se mohl i naučit internetové etice, jak správně zvolit heslo či nakládat s e-maily, a hlavně jak se v online prostředí chovat obezřetně.

V poslední kapitole praktické části pak práce čtenáři poukázala na systémová opatření jako firewall, antiviry či důležitost aktualizací. Dále představila různá důležitá nastavení prohlížečů včetně mnoha jeho užitečných rozšíření a nástrojů. Nakonec pak čtenáře seznámila s technologiemi jako jsou proxy servery, VPN, prohlížeče Tor a Brave nebo operační systém Linux Kodachi speciálně vyvinutý právě pro zachování anonymity uživatele.

Tato práce by měla čtenáři posloužit jako jednoduchý návod, jak nabýt anonymitu na Internetu. Kromě toho by po přečtení této práce měl čtenář získat základní znalosti a obecné povědomí historického pozadí v oblasti Internetu a anonymity. Dále by měl být poučen o hrozbách, kterým musí jeho soukromí každý den na Internetu čelit a jak se jim bránit nebo jim předejít.

SEZNAM POUŽITÉ LITERATURY

[1] BEDNÁŘ, Vojtěch. Co je to Internet?. *Lupa.cz* [online]. 2007 [cit. 2020-03-03]. Dostupné z: https://www.lupa.cz/clanky/co-je-to-internet/

[2] BLAŽKOVÁ, Martina. *Jak využít internet v marketingu: krok za krokem k vyšší konkurenceschopnosti*. 1. vyd. Praha: Grada, 2005. Manažer. ISBN 80-247-1095-1.

[3] SVRŠEK, Jiří. Historie sítě ARPANET/Internet. *Natura.baf.cz* [online]. [cit. 2020-03-03]. Dostupné z: http://natura.baf.cz/natura/2002/3/20020303.html

[4] Jak na Internet. *Cz.nic* [online]. 2014 [cit. 2020-03-03]. Dostupné z: https://www.jaknainternet.cz/page/1205/historie-internetu/

[5] Internet. *Mendelu.cz* [online]. 2013 [cit. 2020-03-03]. Dostupné z: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=40844

[6] Budoucnost Internetu. *Ijs.8u.cz* [online]. [cit. 2020-03-03]. Dostupné z: http://ijs2.8u.cz/index.php?option=com_content&view=article&id=33&Itemid=135

[7] Sociální síť (v sociologii). *ManagmentMania.com* [online]. [cit. 2020-03-03]. Dostupné z: https://managementmania.com/cs/socialni-sit

[8] HISTORIE SOCIÁLNÍCH SÍTÍ. *Socialnisite.estranky.cz* [online]. [cit. 2020-03-03]. Dostupné z: https://socialnisite.estranky.cz/clanky/historie-socialnich-siti.html

[9] PROKŮPEK, Václav. Z historie sociálních sítí. *Txt.cz* [online]. 2012 [cit. 2020-03-03]. Dostupné z: http://vaclavprokupek.ano2012.txt.cz/clanky/102529/z-historie-socialnich-siti

[10] STEVENSON, John. *All you need to know about Darkweb – How to access and what to look out for:: How to access and what to look out for*. John Stevenson.

[11] VÁCLAVÍK, Lukáš. Většina internetu je skrytá. Co jsou to deep a dark web?. *Cnews.cz* [online]. 2018 [cit. 2020-03-03]. Dostupné z: https://www.cnews.cz/co-je-to-deep-invisible-hluboky-dark-temny-web

[12] RUMERO, David. The levels of internet: Surface, Deep and Dark web. *Rumero.co.zw* [online]. 2019 [cit. 2020-03-03]. Dostupné z: https://rumero.co.zw/the-levels-of-internet-surface-deep-and-dark-web/

[13] SHIM, Timothy. Jak získat přístup k tmavému webu: Prohlížení webů Dark Web, TOR Browser a .Onion. *Webhostingsecretrevealed.net* [online]. 2020 [cit. 2020-03-03]. Dostupné z: https://www.webhostingsecretrevealed.net/cs/blog/web-tools/tourist-guide-to-dark-web-accessing-the-dark-web-tor-browser-and-onion-websites/

[14] Pojem anonymita. *Scs.abz.cz* [online]. [cit. 2020-03-05]. Dostupné z: https://slovnik-cizich-slov.abz.cz/web.php/slovo/anonymita

[15] VODÁKOVÁ, Alena. Anonymita. *Sociologická encyklopedie* [online]. 2017 [cit. 2020-03-05]. Dostupné z: https://encyklopedie.soc.cas.cz/w/Anonymita

[16] PAKU, Gillian. Anonymity in the Eighteenth Century. *Oxford Handbooks Online* [online]. 2015 [cit. 2020-03-05]. Dostupné z: https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199935338.001.0001/oxfordhb-9780199935338-e-37

[17] PALME, Jacob. Anonymity on the Internet. *People.dsv.su.se* [online]. [cit. 2020-03-05]. Dostupné z: https://people.dsv.su.se/~jpalme/society/anonymity.html

[18] Anonymous author of The Epic of Gilgamesh. *Editoreric.com* [online]. [cit. 2020-03-05]. Dostupné z: http://www.editoreric.com/greatlit/authors/Author-of-Gilgamesh.html

[19] DALE, Oliver. A History of Cryptography and the Rise of the CypherPunks. *Blockonomi.com* [online]. 2018 [cit. 2020-03-05]. Dostupné z: https://blockonomi.com/cryptography-cypherpunks/

[20] MILHON, Jude. Women in Technology. *Gradiant* [online]. 2019 [cit. 2020-03-05]. Dostupné z: https://www.gradiant.org/en/blog/women-technology-jude-milhon/

[21] KALISKÝ, Boris. *Bitcoin a ti druzí: nepostradatelný průvodce světem kryptoměn*. Praha: IFP Publishing, 2018. ISBN 978-80-87383-71-1.

[22] HUGHES, Eric. A Cypherpunk's Manifesto. *Activism.net* [online]. 1993 [cit. 2020-03-05]. Dostupné z: https://www.activism.net/cypherpunk/manifesto.html

[23] MAYER, Jonathan R. *Internet Anonymity in the Age of Web 2.0* [online]. 7.4.2009. 2009 [cit. 2020-03-05]. Dostupné z: https://jonathanmayer.org/publications/thesis09.pdf

[24] SCHNORR, Andrew. An Anonymous World. *Ocf.berkeley.edu* [online]. 2007 [cit. 2020-03-05]. Dostupné z: https://www.ocf.berkeley.edu/~schnorr/IDS110%20Final%20Project/index.html

[25] Your ISP Is Tracking Every Website You Visit: Here's What We Know. *PrivacyPolicies.com* [online]. 2019 [cit. 2020-03-05]. Dostupné z: https://www.privacypolicies.com/blog/isp-tracking-you/

[26] PETROWSKI, Thorsten. *Bezpečí na internetu: pro všechny*. Vyd. 1. Liberec: Dialog, 2014. Tajemství (Dialog). ISBN 9788074240669.

[27] Anonymity, Privacy, and Security Online. *Pew Research Center* [online]. 2013 [cit. 2020-03-05]. Dostupné z: https://www.pewresearch.org/internet/2013/09/05/anonymity-privacy-and-security-online-2/

[28] RUSSELL, Daniel. THE ANONYMITY IMPOSSIBILITY: STATS, SURVEYS, AND FIGURES. *Attentiv* [online]. 2015 [cit. 2020-03-05]. Dostupné z: http://attentiv.com/anonymity-impossibility/#comments

[29] Anonymita v prostředí internetu. *Wikisofia* [online]. 2013 [cit. 2020-03-05]. Dostupné z: https://wikisofia.cz/wiki/Anonymita_v_prost%C5%99ed%C3%AD_internetu

[30] CAPLAN, J. a J. TORPEY. Identity and Anonymity: Some Conceptual Distinctions and Issues for Research. *Web.mit.edu* [online]. 2001 [cit. 2020-03-05]. Dostupné z: http://web.mit.edu/gtmarx/www/identity.html

[31] Co jsou cookies a k čemu slouží? Je třeba se bát cookies?. *Stawebnice* [online]. 2015 [cit. 2020-03-05]. Dostupné z: https://www.stawebnice.com/seo/seo-blog/co-jsou-cookies-k-cemu-slouzi-cookies/

[32] CARNAGHAN, Ian. Online Anonymity: Good or Bad?. *Carnaghan.com* [online]. [cit. 2020-03-05]. Dostupné z: https://www.carnaghan.com/online-anonymity-good-or-bad/

[33] THE NEGATIVE IMPACT OF INTERNET ANONYMITY. *Mediafactory.org.au* [online]. [cit. 2020-03-05]. Dostupné z: http://www.mediafactory.org.au/2015-media6-deepweb/2015/10/01/the-negative-impact-of-internet-anonymity/

[34] *Bible: překlad 21. století*. 6. opravené vydání. Praha: Biblion z.s., 2019. ISBN 978-80-87282-44-1.

[35] HANIF, Mehmood. What Data Is Collected About You Online and How to Stop It. *Globalsign.com* [online]. 2018 [cit. 2020-03-31]. Dostupné z: https://www.globalsign.com/en/blog/what-data-is-collected-about-you-online

[36] BAILEY, Matthew. *Complete Guide to Internet Privacy, Anonymity & Security*. Nerel, 2011. ISBN 3950309349.

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

[38] How to view your location history in Google Maps. *Androidcentral.com* [online]. 2018 [cit. 2020-04-01]. Dostupné z: https://www.androidcentral.com/how-view-your-location-history-google-maps#view

[39] NAKASHIMA, Ryan. AP Exclusive: Google tracks your movements, like it or not. *Apnews.com* [online]. 2018 [cit. 2020-04-01]. Dostupné z: https://apnews.com/828aefab64d4411bac257a07c1af0ecb/AP-Exclusive:-Google-tracks-your-movements,-like-it-or-not

[40] The Data You Reveal Online: What Websites Collect. *Breadcrumbcyber.com* [online]. 2018 [cit. 2020-03-31]. Dostupné z: https://breadcrumbcyber.com/2018-8-9-the-data-you-reveal-online-what-websites-collect/

[41] Browser Fingerprinting: What Is It and What Should You Do About It?. *Pixelprivacy.com* [online]. [cit. 2020-04-02]. Dostupné z: https://pixelprivacy.com/resources/browser-fingerprinting/

[42] Learn how identifiable you are on the Internet. *Amiunique.org* [online]. [cit. 2020-04-03]. Dostupné z: https://amiunique.org/

[43] Is your browser safe against tracking?. *Panopticlick.eff.org* [online]. [cit. 2020-04-03]. Dostupné z: https://panopticlick.eff.org/

[44] Privacy Analyzer: See what data is exposed from your browser. *Privacy.net* [online]. 2020 [cit. 2020-04-07]. Dostupné z: https://privacy.net/analyzer/

[45] SLÍŽEK, David. *Úniky dat: Hlavní obětí je důvěra lidí v internet* [online]. 2016 [cit. 2020-04-04]. Dostupné z: https://www.lupa.cz/clanky/uniky-dat-hlavni-obeti-je-duvera-lidi-v-internet/

[46] *World's Biggest Data Breaches & Hacks* [online]. 2020 [cit. 2020-04-04]. Dostupné z: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

[47] SWINHOE, Dan. *The 14 biggest data breaches of the 21st century* [online]. 2020 [cit. 2020-04-04]. Dostupné z: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

[48] ';--have i been pwned?. *Haveibeenpwned.com* [online]. 2020 [cit. 2020-04-04]. Dostupné z: https://haveibeenpwned.com/

[49] RFC 1855 - PRAVIDLA CHOVÁNÍ V SÍTI - NETIKETA. *Hoax.cz* [online]. [cit. 2020-04-07]. Dostupné z: https://www.hoax.cz/hoax/netiketa

[50] Google: Zásady bezpečného používání internetu. *Cnews.cz* [online]. 2013 [cit. 2020-04-07]. Dostupné z: https://www.cnews.cz/google-zasady-bezpecneho-pouzivani-internetu/

[51] HORČÍK, Jan. Jak se bránit sledování na každém kroku? Deset tipů pro bezpečný pohyb na internetu. *Zpravy.tiscali.cz* [online]. 2016 [cit. 2020-04-07]. Dostupné z: https://zpravy.tiscali.cz/jak-se-branit-sledovani-na-kazdem-kroku-deset-tipu-pro-bezpecny-pohyb-na-internetu-278289

[52] VANĚK, Jiří, Jiří NOVÁK a David KALIKA. *Jak na Internet bezpečně*. 1. vydání. Ilustroval Aneta BISKUPOVÁ. Praha: CZ.NIC, z.s.p.o., 2018. CZ.NIC. ISBN 978-80-88168-29-4.

[53] HOW SECURE IS MY PASSWORD? ENTER PASSWORD. *Howsecureismypassword.net* [online]. 2020 [cit. 2020-04-07]. Dostupné z: https://howsecureismypassword.net/

[54] The Best Password Managers to Secure Your Digital Life: Keep your logins under lock and key. We picked our favorites for PC, Mac, Android, iPhone, and web browser. *Wired.com* [online]. 2020 [cit. 2020-04-07]. Dostupné z: https://www.wired.com/story/best-password-managers/

[55] 10 Minute Mail: Free Temporary Email. *10minutemail.com* [online]. 2020 [cit. 2020-04-07]. Dostupné z: https://10minutemail.com/

[56] HRUŠKA, Pavel. Jak vypnout automatické aktualizace ve Windows 10. *Mrpear.net* [online]. [cit. 2020-04-25]. Dostupné z: http://www.mrpear.net/cz/blog/749/jak-vypnout-automaticke-aktualizace-ve-windows-10

[57] Windows Update: nejčastější dotazy. *Support.microsoft.com* [online]. 2019 [cit. 2020-04-25]. Dostupné z: https://support.microsoft.com/cs-cz/help/12373/windows-update-faq

[58] Best firewall of 2020 : free and paid software and services. *Techradar.com* [online]. 2020 [cit. 2020-07-08]. Dostupné z: https://www.techradar.com/best/firewall

[59] Top 10 BEST Free Firewall Software For Windows [2020 List]. *Softwaretestinghelp.com* [online]. 2020 [cit. 2020-07-08]. Dostupné z: https://www.softwaretestinghelp.com/best-free-firewall/

[60] TAYLOR, James. Windows Defender Antivirus Review 2020 - Does it Actually Work?. *Safetydetectives.com* [online]. 2020 [cit. 2020-04-25]. Dostupné z: https://www.safetydetectives.com/best-antivirus/windows-defender/?utm_source=youtube&utm_content=defender&utm_term=des

[61] Odstranění nežádoucích reklam, vyskakovacích oken a malwaru. *Support.google.com* [online]. 2020 [cit. 2020-04-26]. Dostupné z: https://support.google.com/chrome/answer/2765944?visit_id=637235021647746324-2233977628&p=chrome_cleanup_tool&hl=cs&rd=2

[62] Smazání historie prohlížení v Chromu. *Support.google.com* [online]. 2020 [cit. 2020-04-26]. Dostupné z: https://support.google.com/chrome/answer/95589?co=GENIE.Platform%3DDesktop&hl=cs

[63] KRÁL, Vojtěch. Anonymní prohlížení, kdy se hodí a kdy ne?. *VojtěchKrál.cz* [online]. 2019 [cit. 2020-04-26]. Dostupné z: https://www.vojtechkral.cz/anonymni-prohlizeni-kdy-se-hodi-a-kdy-ne/

[64] Reklamy Google vás mohou identifikovat a následovat. Jak se odhlásit?. *IDnes.cz* [online]. 2016 [cit. 2020-04-27]. Dostupné z:

https://www.idnes.cz/technet/internet/google-reklamy-zmena.A161023_152249_sw_internet_pka

[65] *Chip: magazín o informačních technologiích*. Praha: Burda Praha s.r.o., 2019. ISSN 1210-0684.

[66] Adblock Plus - free ad blocker. *Chrome.google.com* [online]. 2020 [cit. 2020-04-26]. Dostupné z: https://chrome.google.com/webstore/detail/adblock-plus-free-ad-bloc/cfhdojbkjhnklbpkdaibdccddilifddb?hl=cs

[67] Blokujte reklamy. Prohlížejte Lépe. *Getadblock.com* [online]. 2020 [cit. 2020-04-26]. Dostupné z: https://getadblock.com/

[68] Privacy Badger. *Privacybadger.org* [online]. 2020 [cit. 2020-04-26]. Dostupné z: https://privacybadger.org/

[69] We make powerful privacy solutions used by 350 million people. *Disconnect.me* [online]. 2020 [cit. 2020-04-26]. Dostupné z: https://disconnect.me/

[70] Giving you control of trackers at the device level. *Ghostery.com* [online]. 2020 [cit. 2020-04-28]. Dostupné z: https://www.ghostery.com/?utm_source=ghostery.com&utm_campaign=install_ghostery_hp

[71] *Encrypt the web: Install HTTPS Everywhere today.* [online]. 2020 [cit. 2020-04-26]. Dostupné z: https://www.eff.org/https-everywhere

[72] NoScript 10 "Quantum" resources. *Noscript.net* [online]. [cit. 2020-04-27]. Dostupné z: https://noscript.net/

[73] Clicking ads so you don't have to. *Adnauseam.io* [online]. 2020 [cit. 2020-04-26]. Dostupné z: https://adnauseam.io/

[74] TrackMeNot. *Trackmenot.io* [online]. [cit. 2020-04-26]. Dostupné z: https://trackmenot.io/

[75] Browse the web privately as it was meant to be. *Windscribe.com* [online]. 2020 [cit. 2020-04-28]. Dostupné z: https://windscribe.com/

[76] PETTERS, Jeff. What is a Proxy Server and How Does it Work?. *Varonis.com* [online]. 2020 [cit. 2020-05-07]. Dostupné z: https://www.varonis.com/blog/what-is-a-proxy-server/

[77] Free OpenVPN and PPTP VPN. *Vpnbook.cz* [online]. [cit. 2020-04-28]. Dostupné z: https://www.vpnbook.com/

[78] REZEK, Tomas. NordVPN Recenze (2020) – Je pravda, co se říká?. *Cs.vpnmento.com* [online]. 2020 [cit. 2020-04-28]. Dostupné z: https://cs.vpnmentor.com/reviews/nordvpn/?keyword=nordvpn%20recenze&geo=1003784&device=&ad=394441766551&adposition=&gclid=CjwKCAjwqJ_1BRBZEiwAv73uwEOcG9p0TzGZvxGeh7tWI2IEsUSqAR8j1JKENG_SwQMTup4eSGTXZBoCkvUQAvD_BwE

[79] Online security starts with a click. *Nordvpn.cz* [online]. 2020 [cit. 2020-04-28]. Dostupné z: https://nordvpn.com/

[80] Want to Know Why You Need PureVPN?. *Purevpn.com* [online]. 2020 [cit. 2020-04-29]. Dostupné z: https://www.purevpn.com/why-purevpn

[81] Browse Privately. Explore Freely. *Torproject.org* [online]. 2020 [cit. 2020-05-07]. Dostupné z: https://www.torproject.org/

[82] RUNNING TOR BROWSER FOR THE FIRST TIME. *Torproject.org* [online]. 2020 [cit. 2020-05-07]. Dostupné z: https://tb-manual.torproject.org/running-tor-browser/

[83] You deserve a better Internet. *Brave.com* [online]. 2020 [cit. 2020-05-07]. Dostupné z: https://brave.com/

[84] Kodachi 6.2 The Secure OS. *Digi77.com* [online]. 2013 [cit. 2020-05-08]. Dostupné z: https://www.digi77.com/linux-kodachi/

[85] KUKAČ, Martin. *Linux Kodachi 6.0 - systém pro paranoiky* [online]. 2019 [cit. 2020-05-08]. Dostupné z: https://diit.cz/clanek/linux-kodachi-60-system-pro-paranoiky

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ARPA	Advanced Research Project Agency
ARPANET	Advanced Research Project Agency Network
CSS	Cascading Style Sheets
DNS	Domain Name Systém
FESNET	Federal Educational and Scientific Network
GPS	Global Positioning Systém
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I2P	Invisible Internet Project
IP	Internet Protocol
IRC	Internet Relay Chat
ISP	Internet Service Provider
MILNET	Military Network
NCP	Network Control Program
NSFNET	National Science Foundation NETwork
P2P	peer-to-peer
PPTP	Point-to-Point Tunneling Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
VPN	Virtual Private Network
WWW	World Wide Web

SEZNAM OBRÁZKŮ

SEZNAM TABULEK