Digitální stopa a šedá data

Petr Juračka

Bakalářská práce
2022

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav ochrany obyvatelstva

Akademický rok: 2021/2022

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Petr Juračka**
Osobní číslo:	**L19099**
Studijní program:	**B2825 Ochrana obyvatelstva**
Studijní obor:	**Ochrana obyvatelstva**
Forma studia:	**Prezenční**
Téma práce:	**Digitální stopa a šedá data**

Zásady pro vypracování

1. Zpracujte rešerši vztahující se k dané problematice.
2. Seznamte se s metodami využívanými ke sběru dat a zaznamenávání digitální stopy uživatelů.
3. Proveďte komparaci vybraných anonymizačních služeb a softwarů.
4. Na základě provedené komparace navrhněte opatření pro minimalizaci digitálních stop uživatele.

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

Seznam doporučené literatury:

1. BROOKS, Charles et al.*Cybersecurity Essentials*. John Wiley, 2018. ISBN 978-1-119-36239-5.
2. KOULOUCH, Jan a BAŠTA, Pavel. *Cybersecurity*. CZ.NIC, 2019. ISBN 978-80-88168-31-7.
3. ŠULC, Vladimír. *Kybernetická bezpečnost.* Čeněk, 2018. ISBN 978-80-7380-737-5.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Ing. Petr Svoboda, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání bakalářské práce: **1. prosince 2021**
Termín odevzdání bakalářské práce: **13. května 2022**

L.S.

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 1. prosince 2021

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- 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;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- 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 obsahově totožné.

V Uherském Hradišti, dne: 13. 5. 2022

Jméno a příjmení studenta: Petr Juračka

.....
podpis studenta

ABSTRAKT

V teoretické části této bakalářské práce jsou detailněji rozebrány pojmy šedá data a digitální stopa. Pojem digitální stopa je přiblížen s důrazem, na možnosti zaznamenávání a následné utváření digitální stopy. Samotné digitální stopy se skládají z dat, tedy i z šedých dat. Z toho je následně vycházeno v praktické části, kde jsou zkoumány možnosti, kterými je možné tuto stopu ideálně eliminovat, nebo alespoň snížit. Následně jsou z výsledků porovnání vybraných, volně dostupných nástrojů vypracována doporučení pro uživatele. Tato doporučení mají za cíl přiblížit uživateli internetu možnosti, kterými se je možné, efektivně bránit před záznamem jeho digitální stopy a tím i před vytvořením šedých dat.

Klíčová slova: Bezpečnost, digitální stopa, internet, soukromí, šedá data.

ABSTRACT

In the theoretical part of this bachelor thesis, the terms gray data and digital footprint are discussed in more detail. The concept of digital track is approached with emphasis on the possibilities of recording and subsequent creation of a digital track. The digital tracks themselves consist of data, ie also gray data. This is then followed in the practical part, where the possibilities are examined, which can ideally eliminate this footprint, or at least reduce it. Subsequently, recommendations for users are developed from the results of the comparison of selected, freely available tools. These recommendations aim to bring the Internet user closer to the possibilities that can be used to effectively prevent the recording of their digital footprint and thus the creation of gray data.

Keywords: Digital footprint, gray data, Internet, privacy, security.

Na tomto místě bych rád poděkoval především svému vedoucímu práce, kterým byl pan Ing. Petr Svoboda, Ph.D.. A to především za jeho ochotu, čas a připomínky, kterými mi pomohl v průběhu zpracovávání této práce.

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

OBSAH

ÚVOD

Ne s nadsázkou jsou dnes data, generovaná našimi online aktivitami nazývaná „nové černé zlato“, s odkazem na ropu a její význam ve světě. Data sama osobě, jsou poměrně bezcenná. Nicméně s rozvojem v oblasti datových center, strojového učení a umělé inteligence, nabývají tato data na významu. Dnes je již možné tato data shromažďovat ve velkých objemech. Následně je možné tato nasbíraná velká data levně analyzovat, třídit, využívat, nebo prodávat.

S tím, jak roste možnost data využít ve svůj prospěch, roste i chuť po nich. Kevin Mitnick se ve své knize The Art of Invisibility zaměřil, mimo jiné na největší úniky dat v posledních letech. Jak je vidět s narůstajícím počtem aktivních uživatelů na internetu, jsou i počty lidí, kterých se tyto úniky týkají čím dál početnější. Za zmínku zde stojí uvést několik z nich.

Po úniku dat ve společnosti Equifax, se do rukou útočníků dostaly informace o 145 milionech osob, převážně amerických občanů. Závažnost úniku ve společnosti Exuifax spočívá v tom, že společnost funguje jako registr dlužníků. I proto se únik týkal velmi citlivých osobních údajů typu: jméno, datum narození, adresa, číslo řidičského průkazu, rodné číslo a více než 200 tisíc údajů o kreditních kartách. Dalším významným únikem byl postižen hotelový řetězec Marriott’s Starwood, jemuž byly ukradeny informace z rezervačního systému o více než 500 milionech hostů. Tato uniklá data obsahovala kromě údajů o kreditních kartách, také kontaktní adresy hostů a čísla jejich pasů. (Mitnick, 2019)

Údaje o online aktivitách nemusí ovšem pramenit jen z výše uvedených úniků. Každodenní aktivity na internetu za sebou zanechávají digitální stopu. Data a informace obsažené v této stopě je možné následně využít. Ať už cíleným marketingem, předvídáním chování uživatele, nebo jen prodáváním těchto informací.

Je tedy nutné si položit otázku, zda jsou naše online aktivity tak soukromé, jak si myslíme. A pokud tedy naše online aktivity nejsou tak soukromé, jak si myslíme, zda je možné s tím něco udělat.

Hlavním cílem této práce je tedy definice přístupů uživatele k problematice digitální stopy a šedých dat. Hlavní cíl bude naplňován za pomocí 4 dílčích cílů. Prvním dílčím cílem je rešerše problematiky digitální stopy a šedých dat. Druhým dílčím cílem je komparace vybraných webových prohlížečů z hlediska správy digitální stopy. Třetím dílčím cílem je provedení komparace nástrojů pro správu digitální stopy uživatele. Posledním, čtvrtým dílčím cílem je poté návrh a sumarizace možných přístupů a opatření uživatele pro správu

jeho digitální stopy. Z hlediska omezení práce, se tato zaměřuje jen na počítače s operačními systému Windows 7 a novějšími.

I. TEORETICKÁ ČÁST

1 ŠEDÁ DATA

V otázce šedých dat se setkáváme s mnoha přístupy k definici, co to šedá data jsou. Pro potřeby této práce si zde rozebereme 5 základních přístupů:

- Data v kontextu teorie šedých systémů
- Anonymní data definovaná podle EU
- Nestrukturovaná data
- Neřízená nebo riziková data
- Syntetická data

1.1 Teorie šedých systémů

Tuto teorii zpopularizoval Julon Deng v roce 1982. (Savíc, 2019) V této době se mu podařilo vyvinou metodologii, která se zaměřovala na studii problémů, zahrnujících nedostatečné množství dat a špatné informace, což je velmi častou situací v oborech jako ekonomie, finance, politika a další. Na tento výzkum navazovala práce kolektivu Siefen Liu, Jeffrey Forrest, Yingjie Yang (2017), kde byly představeny základní metody, modely a techniky pro praktické využití analýzy šedých dat. Zde taktéž byla data rozdělena do několika kategorií. Jednalo se o dělení na bílá data, šedá data a černá data. Bíla data představují informace kompletně známá, šedá data představují částečně známé a částečně neznámé informace a černá data představují informace neznámé. Přesněji se dá říct, že šedá data představují malé vzorky dat nevalné kvality, které jsou často jen z části známy, nekompletní nebo nepřesné. (Savíc, 2019)

1.2 Šedá data podle Evropské Unie

Evropská Unie pohlíží na anonymní data jako na typ šedých dat a pracuje s nimi jako s právním termínem v případě EU General Data Protection regulation (GDPR). (Savíc, 2019) Hlavní starostí tohoto zákona v souvislosti s šedými daty bylo další využívání osobních dat za jiným než původním účelem. Nicméně je důležité si uvědomit, že se toto vztahuje jen na data, která mohou identifikovat konkrétní osobu. Anonymní data nejsou považována za osobní a jsou tedy mimo dohled GDPR. To s sebou přináší problém v otázce použití technik, která data de-anonymizují. V tomto případě se jedná především o použití

pseudo identifikátorů typu: věk, pohlaví, vzdělání, zaměstnání, rodinný status, mateřský jazyk a další. (Savíc, 2019)

GDPR pracuje s pseudo-anonymními daty tak, jako by byla osobní. Například data, která využívají přiřazené identifikátory, které by umožnily spojit si data s konkrétním účastníkem (například u výzkumů). Proto je podle GDPR vyžadováno odstranění možných identifikujících údajů, a to takovým způsobem, aby nebylo možné data de-anonymizovat ani například zkombinováním anonymních dat s daty z jiných zdrojů.

Evropská unie taktéž vyžaduje princip minimalizace. Jinými slovy je možné sbírat jen co nejmenší množství osobních dat, která jsou potřebná. Důsledkem této politiky nicméně je to, že většina dat, která jsou takto nasbírána, patří do kategorie šedých dat. (Savíc, 2019)

1.3 Nestrukturovaná data

Nestrukturovaná data reprezentují všechna data, která nemají danou a rozpoznatelnou strukturu. Jsou to tedy data, která kvůli absenci struktury nejsou vhodná pro použití do databází. Zde si můžeme představit například textové soubory, emailové zprávy, powerpointové prezentace, výsledky dotazníků, příspěvky na blogu, obrázky na sociálních sítích, data ze senzorů a další. (Savíc, 2019)

Nicméně s rozvojem informačních technologií a nástrojů, jako jsou umělá inteligence, strojové učení, prediktivní analýza nebo těžba dat, jsou tato nestrukturovaná data efektivně třízena, klasifikována a kategorizována. Hranice mezi strukturovanými a částečně strukturovanými daty je jen velmi tenká, a i v případě nestrukturovaných dat, jednoduše pomocí přidání tagů metadat se tato data stávají částečně strukturovanými, nebo dokonce plně strukturovanými. (Savíc, 2019)

1.4 Neřízená nebo riziková data

Tento typ dat představuje podle některých odhadů až 30 % všech korporátních dat. Dalších 30 % je zaplněno aktivními daty a zbytek jsou neaktivní data určená pro archivační účely. (Savíc, 2019) Z těchto 30 % neřízených dat, 10 % jsou data ztracená, nebo která už dávno měla být odstraněna a 5 % jsou data osobní, která nemají na korporátních serverech ve volné podobě existovat. Tato data mohou znamenat značná rizika z důvodu možného zneužití osobních údajů. (Savíc, 2019)

1.5 Syntetická data

Syntetická data jsou považována za nejmladší část šedých dat. Jsou specifická v tom, že jsou uměle vytvořená. Tato syntetická data jsou většinou anonymizována (odstraněním identifikačních aspektů jako například jméno, e-mail, adresa atd.) a vytvořena podle požadavků tak, aby připomínala data reálná. Tato data jsou totiž důležitým nástrojem pro strojové učení a je možné je používat, pokud jsou reálná data buď příliš drahá, nebo je nemožné. je z důvodu bezpečnosti sbírat a využívat, popřípadě pokud jsou reálná data neúplná. (Savic, 2019)

S vývojem systémů umělé inteligence a pokroku v informačních technologiích se očekává, že hranice mezi syntetickými a reálnými daty prakticky vymizí. Je to dáno i tím, že systémy umělé inteligence, které se dokáží učit z dat reálných, jsou také schopny na základě tohoto učení vytvářet data syntetická, které připomínají data reálná. Společnost Waymo, kterou vlastní společnost Alphabet, testuje autonomní provoz vozidel. Tento systém byl testován na 12 milionech kilometrech v reálném provozu na silnici, ale i na 8 miliardách kilometrech v simulovaném provozu. Provádět testy za pomocí syntetických dat je výrazně levnější a rychlejší. Tento případ ukazuje i význam syntetických dat pro použití v reálném životě. (Savic, 2019)

1.6 Problémy s šedými daty

Při práci s šedými daty vyvstávají dvě hlavní otázky – první ohledně samotných dat a druhá ohledně účelu, za kterým byla data vytvořena.

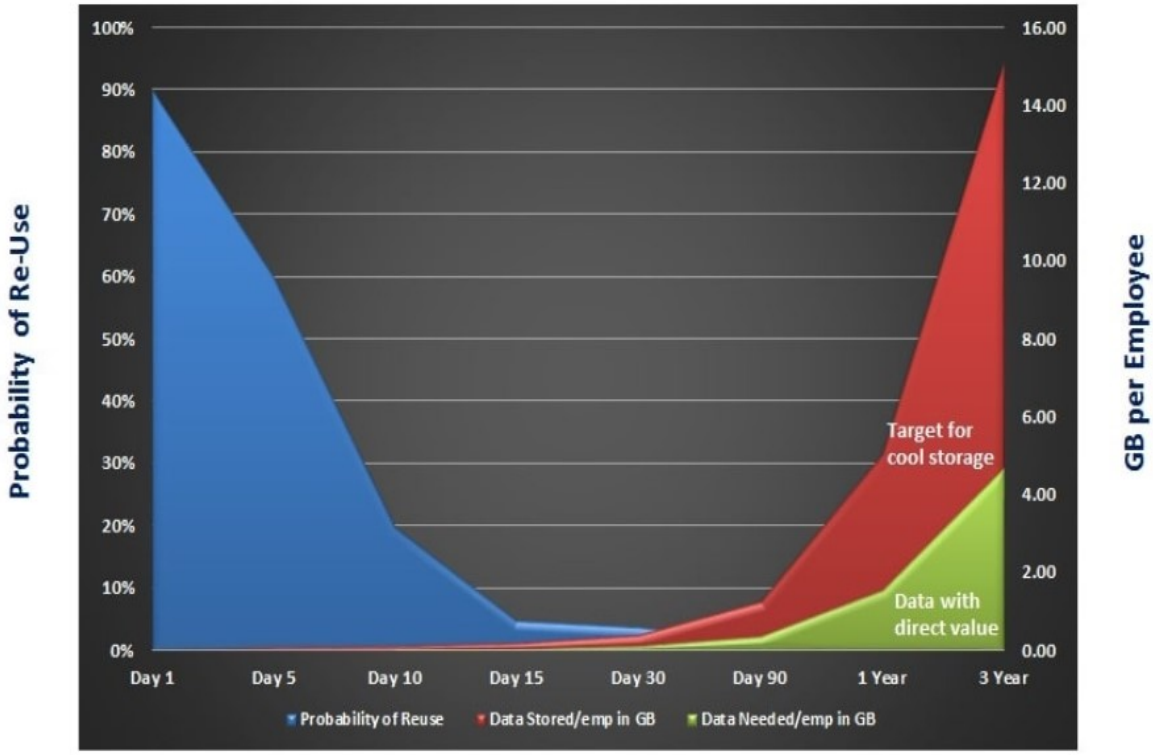
Problém se samotnými šedými daty spočívá v jejich podstatě. A to, že šedá data jsou neověřitelná a přístupná bez jakékoliv garance o jejich správnosti. Nebezpečí zde spočívá v nemožnosti si data ověřit. To může vyústit v použití nepřesných data nebo falešných dat. Spolu s nejasnou strukturou šedých dat a často i šifrováním je použití šedých dat problematické.

Druhý problém souvisí se samotným vznikem dat. Ten může hrát důležitou roli při posouzení důvěryhodnosti obsažených informací. Jako jednoduché pravidlo zde platí, využití dat jen z ověřených zdrojů. U pochybných zdrojů si nemůžeme vzhledem k nemožnosti si data ověřit být jisti úmyslem, za kterým byla tato data vytvořena. (Savic, 2019)

1.7 Životní cyklus informací – od aktivních dat k šedým datům

Dle Freda Moora, který se ve své práci zabýval životním cyklem informací, je životní cyklus informací prakticky stejný bez závislosti na původu. Dle jeho teorie, jak informace stárne, šance na její znovupoužití, a tedy i její hodnota rapidně klesá. Jakmile stáří informace dosáhne 15-30 dní, šance, že bude informace znovu použita se blíží 1 %. Jak informace dále stárne, se tato šance blíží nule, ač se na ní nikdy zcela nedostane. (Tolson, 2016)

Průměrný zaměstnanec se podílí na vytvoření zhruba 20 MB dat každý den. Za 15 pracovních dnů tedy 220 MB a za tři roky se množství vytvořených dat vyšplhá na 15.12 GB. (Tolson, 2016) Podle průzkumu provedeného (CGOC) Compliance, Governance and Oversight v roce 2012, 69 % všech dat, která jsou zaměstnancem uložena by mohla být odstraněna, bez toho, aby to jakkoliv poškodilo společnost. Realita je ovšem taková, že data jsou i nadále udržována především z důvodu, že by v případě budoucího soudního sporu bylo na toto mazání dat pohlíženo, jako na odstraňování důkazů. (Tolson, 2016)



Obr. č. 1 – Životní cyklus informací (zdroj: https://www.archive360.com/blog/the-lifecycle-of-grey-data)

1.8 Šedá data v univerzitním prostředí

Univerzitní prostředí je třetím největším sektorem, co se týče úniku dat. Kdy z celkového množství představují úniky z univerzit zhruba 10 %. Jediné další oblasti s větším únikem dat jsou zdravotnictví a obchod. Od roku 2005 do roku 2017 univerzity nahlásily okolo 800 úniků dat, které postihly celkem více než 25 milionů záznamů. (Borgman, 2018)

Důvodem tak velkého počtu útoků je především větší zranitelnost než v případě bank, zdravotnictví, vládních serverů nebo byznysu. Častým cílem jsou technické univerzity. Ty především z důvodu krádeže výsledů pokročilých výzkumů pro budoucí využití, nebo zneužití. V případě univerzit s vlastním lékařským zařízením, jde útočníkům především o data pacientů, včetně údajů osobních. Stejně tak se i studenti sami stali vyhledávaným cílem těchto útoků z důvodu krádeže přihlašovacích údajů, které mohou být následně využity pro přihlašování se k drahým službám nebo uplatňování studentských slev. (Borgman, 2018)

2 DIGITÁLNÍ STOPA

Data, ze kterých se následně vytváří digitální stopa mohou pocházet prakticky z jakéhokoliv zařízení s přístupem na internet. Už to nejsou jen počítače, jako tomu bylo v minulosti. Dnes o nás naopak sbírají nejvíce informací naše chytré telefony. To ovšem ani v nejmenším neznamená, že množství dat zaznamenávané z ostatních zdrojů by bylo bezvýznamné. (Fish, 2013)

Naopak se pojem digitální stopa objevuje stále častěji, stejně tak i hlasy, volající po její ochraně. Je to způsobeno přesunem běžných aktivit z off-line světa na internet. Dnes už se prakticky vše od nákupů, vyhledávání hotelu, přihlášky ke studiu a hledání řešení problémů provádí online. Tyto aktivity ovšem za sebou zanechávají data, která následně utváří digitální stopu. S tím, jak se zvyšuje výpočetní síla, se i současně zvyšují i možnosti, jak sbírat a ukládat data o tom, co který uživatel dělá. Spolu s vývojem strojového učení začalo být možné automaticky analyzovat tato data ve velkém měřítku a utvářet tak osobnostní profily jednotlivých uživatelů. (Pavlenko, Barykin, Dadteev, 2021)

Digitální stopy mohou nabývat několika podob:

1. Digitální stopy viditelné na internetu i pro ostatní uživatele:
    a. Aktivita na sociálních sítích.
    b. Komentáře pod příspěvky, články nebo diskuse na fórech.
    c. Vlastní internetové stránky, nebo blogy.
2. Digitální stopy neviditelné:
    a. Log soubory na serveru.
    b. Emailové hlavičky.
3. Off-line „digitální“ stopa:
    a. Metadata – strukturovaná data popisující jiná data (setkáme se s nimi například u fotografií, kdy z nich zjistíme nejen místo a čas pořízení, stejně tak i další informace tykající se například fotoaparátu a jeho nastavení pro danou fotku). (Žažo, 2015)

2.1 Definice digitální stopy

Až na forenzní vědy není pojem digitální stopa definován. Všeobecně se za digitální stopy považují data, nebo metadata, která vznikají během interakce uživatele a internetu

(digitálního prostředí). Pro lepší pochopení významu si zde přiblížíme pojetí digitální stopy ve třech odlišných oborech.

V oboru kriminalistiky a forenzních věd je na digitální stopy pohlíženo jako na důkazní materiál. V zahraničí se proto odlišují dva pojmy, a to digital footprints (digitální stopy) a digital evidence (digitální důkazy). U nás se nicméně používá jen pojem digitální stopy, a to i v odborné literatuře. (Skoček, 2012) Ani pokud na digitální stopy pohlížíme z pohledu kriminalistiky nebo forenzních věd, se nemusí jednat jen o dokazování trestného činu. Naopak se forenzní šetření využívá při auditech, ať už v komerční nebo státní sféře. Vychází to i z dnes využívané definice pracovní skupiny SWGDE (Scientific Working Group on Digital Evidence), dle které je digitální stopa „*Informace s vypovídající hodnotou, uložená, nebo přenášená v digitální podobě*“. Mohou mezi ně patřit GPS souřadnice, výpisy hovorů, záznamy z bezpečnostních kamer, ale i metadata u fotografií (Skoček, 2012).

Druhou oblastí, kde jsou intenzivně využívány digitální stopy je marketing. Zde ovšem neexistuje přesná definice. Využívány jsou především v oblasti behaviorálního marketingu. Tento typ marketingu je postaven na sledování chování uživatelů. Tyto údaje jsou analyzovány a je z nich vytvořen profil uživatele, umožňující lepší a efektivnější zacílení reklamy. Toho se dosahuje především sledováním klíčových slov, ať už zadávaných do vyhledávačů, sociálních sítí nebo jiných zdrojích. Dalším aspektem, který se sleduje je pohyb po webových stránkách. Zde se sleduje, nejen navštívená stránka, ale i celková doba navštívení, pohyb po webu, pohyb kurzoru a čas strávený například u určitého objektu. V závislosti na množství nasbíraných dat, je následně utvořen profil uživatele pro komerční účely. (Skoček, 2012)

Třetí oblastí, kde se setkáváme s digitální stopou jsou počítačové vědy. S nástupem internetu a jeho rozšířením mezi populaci začal každý uživatel vytvářet svou digitální stopu. Tuto digitální stopu tvoří soubor dat (informací), které svým pohybem na internetu uživatel zanechává. Toto zanechávání stop může být buď vědomé nebo nevědomé, podle toho se také dělí na dvě skupiny – pasivní digitální stopa a aktivní digitální stopa. (Skoček, 2012)

2.2 Pasivní digitální stopa

Pasivní digitální stopou nazýváme data získaná bez uživatelova souhlasu nebo vědomí.

2.2.1 Možnosti záznamu v off-line prostředí:

1) Logy – Soubory přístupné jen administrátorům (uživatel nezjistí co přesně se loguje).

2) Keylogger – Zaznamenává všechny znaky napsané na klávesnici. Historie použití keyloggerů sahá až do 70. let minulého století. Jeden z nejznámějších prvních incidentů se odehrál v polovině 70. let, kdy sovětští špioni vyvinuli hardwarový keylogger, který se zaměřoval na psací stroje IBM Selectric, používané na amerických ambasádách v Petrohradě a Moskvě. Tento typ hardwarového keyloggeru pracoval na principu měření změny v magnetickém poli psacího stroje v závislosti na otáčení psací hlavy při psaní jednotlivých znaků. Boom v použití keyloggerů nicméně nastal v 90. letech minulého století, kdy se na trh dostaly tisíce typů keyloggerů pro komerční použití. (History of Keyloggers, 2022)

Keyloggery se dělí na 4 základní kategorie.

1. Hardwarový keylogger – Fyzické zařízení, které se instaluje (vkládá) mezi klávesnici a počítač anebo popřípadě přímo do klávesnice.
2. Akustický keylogger – Zaznamenává zvuky jednotlivých stisků kláves. K záznamu se používají parabolické mikrofony, a to až na vzdálenost několika metrů.
3. Bezdrátové keyloggery – Tento typ keylogerů zneužívá technologii Bluetooth a dokáže zaznamenávat data až na vzdálenost několika desítek metrů.
4. Softwarové keyloggery – Nejpoužívanější typ keyloggerů, který zaznamenává data cestující mezi klávesnicí a operačním systémem. Záznam stisknutých kláves se následně ukládá do logu (Abukar, Aizaini, 2014).

2.2.2 Možnosti záznamu v on-line prostředí:

1) Server logy – Textový dokument obsahující všechny aktivity na daném serveru. Jsou automaticky vytvářeny a udržovány na serveru po určitou dobu. Většinou po dobu 30 dní, nebo do určité velikosti. Jsou ukládány primárně kvůli potřebě dohledat podstatu problému, pokud se na serveru vyskytne. (Server Log Files in a Nutshell, 2020) Každý řádek v logu představuje jeden požadavek na server a obsahuje informace:

1. IP adresa odkud přichází požadavek.

2. Identifikaci zařízení, ze kterého přichází požadavek (operační systém, jazyk systému, typ a verze prohlížeče…).
3. Čas a datum požadavku.
4. Požadovanou stránku, kterou chtěl uživatel navštívit.
5. HTTP status kód (možné chybové hlášky).

2) HTTP cookies – malý textový soubor uložený v uživatelově počítači (přístroji) obsahující například uživatelské jméno a heslo. Data v cookies jsou vytvořena po spojení se serverem a označena specifickým identifikátorem pro dané zařízení. Server si při každé další návštěvě ze stejného zařízení přečte informace obsažené v cookies. Ty jsou následně využity k identifikaci použitého přístroje, údajů a nastavení. HTTP cookies můžeme rozdělit podle vlastností na jednorázové a trvalé cookies. Jednorázové cookies jsou využívány pouze pro pohyb na stránce, až do opuštění stránky. Tento typ cookies je ukládán jen v mezi paměti serveru a není zaznamenáván na hard disk. Po opuštění stránky je tento typ cookies vymazán. Hlavním účelem cookies tohoto typu je usnadnění pohybu po stránce, jako je například tlačítko zpět, nebo funkčnost anonymizačních pluginů pro prohlížeč. V případě trvalých cookies je jejich obsah již ukládán na hard disku napořád. Mohou nicméně obsahovat i takzvané datum expirace, které je automaticky vymaže. Hlavním využitím tohoto typu cookies jsou 2 případy: (What are Cookies, 2022)

1. Ověřování – cookies sledují, zda je uživatel přihlášen a pokud ano pod jakým jménem. Jsou využívány také k automatickému vyplňování údajů, aby je uživatel nemusel při každé návštěvě zadávat znovu.
2. Sledování – Tento typ cookies umožnuje sledovat návštěvu uživatele při opakovaných návštěvách. To umožňuje postupně vytvářet osobní profil každého uživatele a navrhovat mu obsah, který ho zaujme. V případě online obchodů to mohou být například věci, které by si zákazník mohl chtít koupit, v případě streamovací služby typu Netflix, například i další seriál podle preferencí uživatele. (What are Cookies, 2022)

Je nutné také rozlišovat kdo dané cookies vytvořil. V základu se dělí na dva typy – cookies první strany a cookies třetí strany. V případě cookies první strany je tvůrce shodný s provozovatelem serveru. Cookies první strany jsou proto považovány za bezpečnější a jejich hlavním účelem, je zjednodušit a zpříjemnit uživateli pobyt na dané webové stránce.

Použití mají v e-shopech, kde umožnují personalizovat nákup, ukládají položky v košíku i bez toho, aby bylo nutné se na dané stránce registrovat. (Hillson, 2021)

Na druhé straně, cookies třetích stran jsou provozovány někým jiným než provozovatelem serveru. Toho je dosaženo pomocí skriptů nebo tagů. Tyto cookies třetích stran již představují pro uživatele větší nebezpečí. Jejich hlavním účelem je o uživateli sbírat informace napříč internetem, primárně ke komerčním účelům. I to je důvod, proč už dnes některé webové prohlížeče umožnují blokovat cookies třetích stran. (Hillson, 2021)

Speciálním typem cookies třetích stran jsou takzvané zombie cookies. Tento typ cookies je trvale nainstalován na uživatelově počítači. A to i když uživatel odmítne cookies přijmout. Tento typ cookies je velmi těžké odstranit i proto, že po odinstalování se znovu automaticky objeví. Někdy je tento typ nazýván také „flash cookies“. (What are Cookies, 2022)

3) Webové chyby – Zneužití internetových chyb na webových stránkách, nebo emailových službách.

4) Historie internetového prohlížeče – Autor prohlížeče může do softwaru zabudovat funkci, která ukládá data o uživateli a následně je odesílá na požadovaný server k dalšímu zpracování, nebo zneužití. (Žažo, 2015)

2.3 Aktivní digitální stopa

Do aktivních digitálních stop patří stopy, které uživatel úmyslně vytváří, za účelem sdílení informací. Jedná se o sdílení pomocí sociálních sítí nebo blogů. Tyto stopy je možné dále dělit, podle prostředí, kde byly vytvořeny. (Kovářová, 2019)

Off-line prostředí:

- Data uložená v souboru (textový soubor, pdf).
- Metadata souborů, o nichž uživatel ví.

On-line prostředí:

- Viditelná aktivita – příspěvky, komentáře.
- Sdílení informací na sociálních sítích (fotky, údaje).
- Vlastní internetové stránky.
- Fóra – z registrace na fórum lze vyčíst zájmy a koníčky.
- Komunikace – chaty, emaily.

Jiné dělení dle potenciálních dopadů na zneužité údaje obsažené v digitálních stopách nabízí například Král:

> *„Červená – rodné číslo, číslo pojištění, identifikační čísla (PIN) účtů, rodné jméno matky, informace o zdravotním stavu, trestní rejstřík, podrobné informace o financích, cestovní plány, seznam předchozích zaměstnání, informace o rodině a přátelích vč. jejich telefonních čísel, e-mailových i skutečných adres atp.*
>
> *Oranžová (žlutá) – telefonní číslo, adresa, datum narození, stav, zaměstnavatel, vzdělání, e-mailová adresa, oblíbené nákupy, číslo kreditní karty, zájmy a koníčky, spolky a sdružení, navštívené WWW stránky apod.*
>
> *Zelená – směrovací číslo, věk, přibližná výše platu, povolání, průzkumy veřejného mínění atd., pokud tyto informace nejsou ve spojení s jinými, choulostivějšími údaji z předchozích skupin.“* (Král, 2006)

2.4 Digitální identita

Digitální identita je ve své podstatě velmi podobná identitě z fyzického světa. Dnes se již smazávají rozdíly i ve fyzickém rozměru identity, který dříve chyběl. S nástupem technologií umožňující použití otisků prstů pro odemykání zařízení, nebo rozpoznávání obličeje se hranice mezi klasickou a digitální identitou smazává. (Skoček, 2015)
Tento proces budování digitální identity je založen na shromažďování vstupů. (Fish, 2013)

Pozornost:

- Data o tom, co uživatel dělá, jaké služby a aplikace využívá.
- Informace o době, po kterou byly aplikace spuštěné, jak dlouho se uživatel díval na fotografii, jakou hudbu a jak dlouho a jak často poslouchal.
- Data o tom, jak tráví uživatel svůj čas v online prostředí.

Poloha:

- Datové záznamy o tom, kde se uživatel nacházel, nebo nachází.
- Jaká místa obvykle navštěvuje a v jakou dobu.
- V případě shromáždění více informací i s kým se na daných místech mohl potkávat (podle informací o poloze jiných uživatelů).

Vyhledávání:

- Informace o vyhledávaných slovních spojeních (i vyhledávání pomocí hlasu).

- Informace tohoto typu dokážou říci mnoho o záměrech uživatele podle vyhledávaných spojení.

Obsah:

- Informace o obsahu, který uživatel vytvořil – text, video, fotka, prezentace, blog nebo příspěvek na sociální síti. (Fish, 2013)

Nasbíraná vstupní data jsou následně analyzována. Pro kvalitnější výstupy je toto třídění a následná analýza prováděná ve smyčce. Ta slouží primárně pro vytřídění nepodstatných informací. Z následných vytřízených dat jsou zpracovány možné výstupy. (Fish, 2013)

Záměr:

- Poskytuje předpověď o uživatelových krocích do budoucna.
- Vytváří se na základě toho, co uživatel dělal, řekl, nebo naznačil, že bude dělat.
- Může vycházet z údajů z kalendáře, e-mailu, informací z vyhledávače, informací ze sociálních sítí.

Doporučení:

- Na základě uživatelovy digitální stopy e možné provést doporučení o stávajícím nebo novém produktu nebo službě.
- Díky informacím je zde vyšší míra pravděpodobnosti, že doporučení bude relevantní.

Ochrana:

- Nasbíraná data mohou sloužit i k ochraně uživatele.
- Nasbíraná data jsou totiž dobrým vodítkem, zda informace, které jsou zadávány, zadává opravdu uživatel, nebo někdo, kdo se za něj jen vydává. Vychází i z principu, že uživatelé mají své zvyky a jen málokdy je mění.
- V tomto případě může jít například o zablokování podezřelé transakce.

Personalizace:

- Aplikace, nebo služby se mohou přizpůsobovat pro konkrétního uživatele.
- Na základě známých informací o uživateli dojde k automatické úpravě. (Fish, 2013)

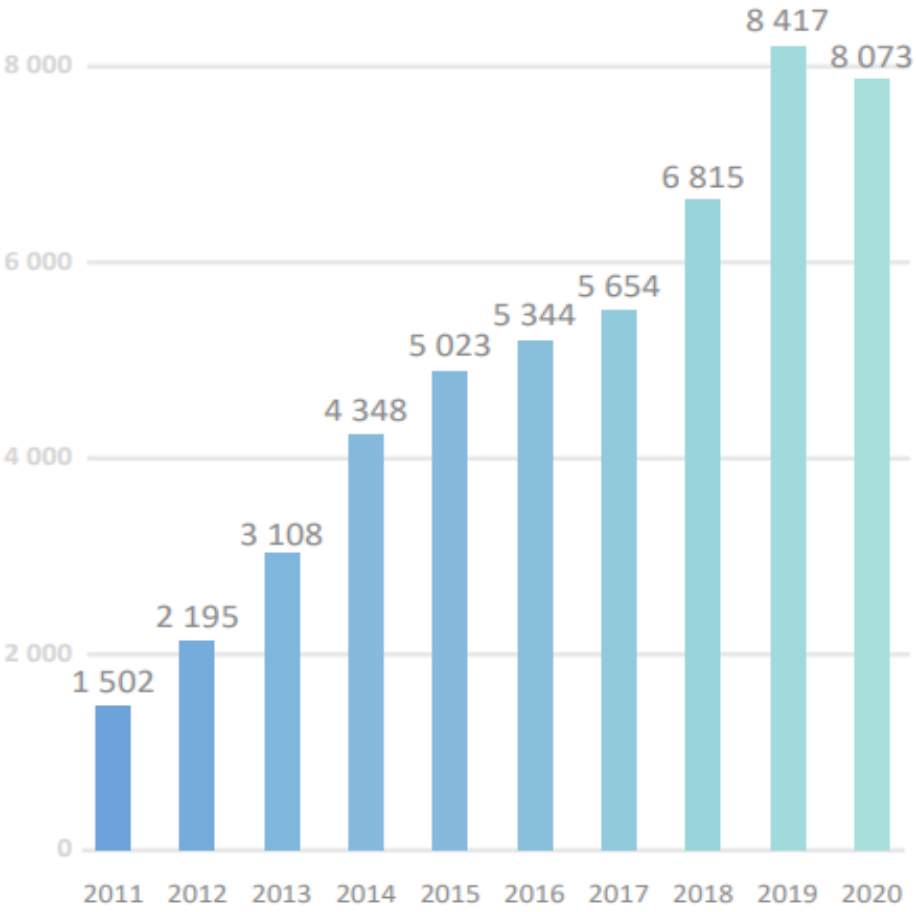
3 KYBERNETICKÉ HROZBY V SOUVISLOSTI S DIGITÁLNÍ STOPOU A ŠEDÝMI DATY

Možností, jak se dostat k cizím údajům je mnoho. Většina z nich nicméně pracuje na dvou principech. Zaprvé je to nedokonalost softwaru, se kterým uživatel pracuje a zadruhé je to nepozornost uživatelů při práci s počítačem, kde se zneužívá, buď nepozornosti, nebo neznalosti uživatelů.

Ze zprávy „Data Breach Investigation Report“ z roku 2017 vyplývá, že 68 % útoků je odhaleno až po několika měsících. (Kolouch, Bašta, 2019) Ze zprávy o stavu kybernetické bezpečnosti České republiky za rok 2020 vydané Národním úřadem pro kybernetickou a informační bezpečnost je možné vyčíst nejen nejčastější způsoby provedení útoků, ale také počet provedených útoků za rok 2020.

- Počet trestných činů v oblasti kybernetické kriminality řešený Policií ČR – **8073**
- Počet bezpečnostních incidentů řešených (CSIRT.CZ) národním bezpečnostním týmem České republiky - **1267**
- Nahlášení kybernetických incidentů NÚKIB - **468**
- Počet kybernetických incidentů řešených NÚKIB - **99**
- Nejčastější cíle incidentů řešených NÚKIB:
    - Státní správa – **43** cílů
    - Zdravotnictví – **16** cílů
    - Finanční instituce – **7** cílů
    - Obce – **7** cílů
    - Doprava – **6** cílů
    - Digitální infrastruktura – **5** cílů
- Nejčastější způsob provedení při incidentech řešených NÚKIB:
    - Škodlivý kód (virus, červ, trojský kůň) – **37** útoků
    - Narušení dostupnosti (DDOS útok, sabotáž) – **26** útoků
    - Průnik (do uživatelského účtu nebo aplikace) – **16** útoků

- Phishing – **7** útoků (Národní úřad pro kybernetickou a informační bezpečnost, 2021)



Obr. č. 2 Počet vyšetřovaných kyberkriminálních případů
v České republice mezi lety 2011 až 2020
(zdroj: Národní úřad pro kybernetickou a informační bezpečnost, 2021)

3.1 Útoky založené na sociálním inženýrství

Sociální inženýrství je využití psychologické manipulace k získání osobních informací, nebo k provedení určité činnosti. Základními prvky, které sociální inženýrství využívá jsou lidské vlastnosti jako stres, důvěra nebo chamtivost. Tyto útoky zneužívají mnohdy nejslabší článek bezpečnosti při použití internetu, a to lidský úsudek. (Green, 2021)

Phishing

Tento typ útoku je založen na emailové komunikaci, kdy se zločinec vydává za někoho jiného. Často předstírají, že jsou zaměstnanci banky, úřadů, doručovací služby, nebo například i nadřízený ve společnosti. Většinou někoho, ke komu máme důvěru. Jejich cílem

je, aby si uživatel otevřel, nebo stáhl přílohu emailu obsahující škodlivý software. Cílem může být také přesvědčit uživatele, aby kliknul na přiložený odkaz, směřující na sice stejně vypadající, ale falešnou stránku, například banky a zadal zde své přihlašovací údaje. Tyto údaje následně mohou být útočníkem snadno zneužity. (Green, 2021)

Phishingové útoky mohou mít různé podoby:

- Pozměněné jméno: Útočníci zneužívají nepozornosti uživatelů při kontrole adresy odkazu, nebo emailové adresy, ze kterého byl email poslán. Emailová adresa může vypadat naprosto stejná jako od oficiální organizace, ale jen s pozměněným písmenem, nebo přidaným znakem a podobně. Ve výsledku se tváří jako oficiální email, čímž vzbuzuje pocit pravosti.
- Připojený odkaz: útočníci připojí odkaz na stránku, pod různými záminkami. Cílová stránka může vypadat identicky se stránkou reálnou a jedinou změnu, kterou uživatel může zpozorovat, je drobná změna v adrese. Zde po uživateli požadují zadat své přihlašovací údaje, které jsou následně zneužity.
- Emailová příloha: v tomto případě je cílem útočníků, aby uživatel kliknul a otevřel přílohu emailu. Mnohdy se maskuje jako potvrzení objednávky, pozvánka na akci a podobně.
- Angler phishing: cílem tohoto útoku je využití sociálních sítí k sociálnímu inženýrství. Jako příklad je možné uvést sledování účtů společností, kdy útočníci oslovují uživatele, kteří si zde stěžovali na produkt. Vydávají se za pracovníky dané společnosti ve snaze napravit daný problém. Během procesu se snaží získat citlivé informace, jako hesla, čísla účtu atd.
- Spear phishing: Tento typ útoku je na rozdíl od klasického phishingu zaměřen na jednotlivce nebo malé skupiny. Zde se snaží vydávat za osobu ke které má uživatel důvěru. Osoba blízká nebo za nadřízený. Tento typ útoků je těžší na provedení, nicméně má vyšší míru úspěšnosti, kdy při komunikaci s osobami, kterým věříme jsme méně ostražití. (Green, 2021)

3.2 Malware

Malware neboli „škodlivý software“ je pojem, pod který patří jakýkoliv škodlivý program nebo kód, ať už škodlivý pro zařízení, nebo systém. Jeho cílem je napadnout, poškodit, nebo

vyřadit z provozu zařízení, přesněji jeho operační systém. Tento útok může zařízení poškodit buď kompletně, nebo jen částečně. (Šulc, 2018)

Motivů k takovému útoku bývá mnoho. Nejčastěji se jedná o finanční zisk nebo o snahu o poškození systému. I když, až na výjimky malware nemůže poškodit zařízení fyzicky, může ukrást, zašifrovat nebo vymazat data. Změnit nebo poškodit základní funkce zařízení a sbírat data na zařízení bez uživatelova vědomí. (Malware, 2022)

Nejčastějšími možnostmi, jak se malware dostane do zařízení je skrze prohlížení webových stránek anebo skrze e-mail. Při prohlížení webových stránek hrozí riziko v případě, že infikovaných stránek, nebo v případě bezpečných stránek, pokud obsahují reklamu se škodlivým kódem. Další možností je stáhnutí a instalace programů a aplikací od neověřeného poskytovatele. V případě e-mailové komunikace se jedná primárně o stažení a otevření infikované přílohy. (Malware, 2022)

Formy malware:

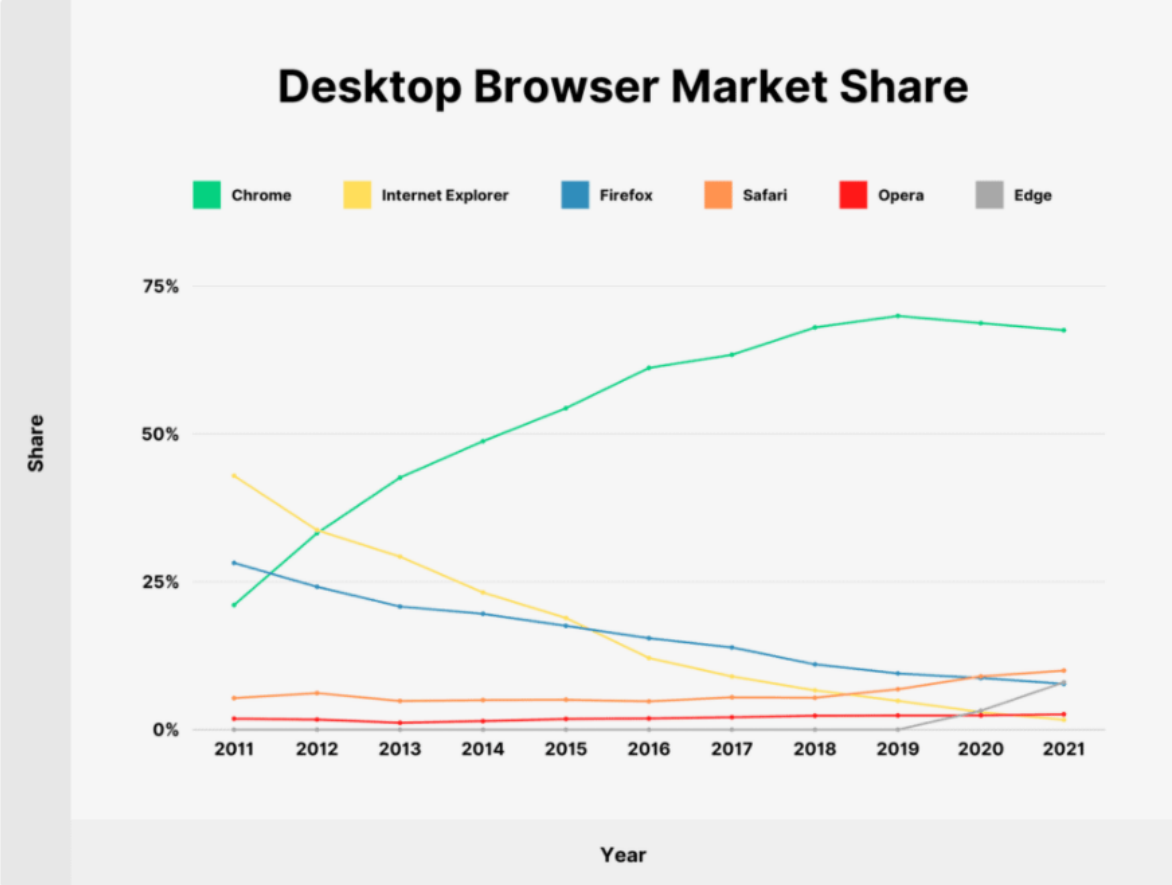
- Adware – Nechtěný software navržený pro vyskakování nechtěných reklam na zařízení. Nejčastěji se tyto reklamy objevují uvnitř prohlížeče. (Malware, 2022)
- Spyware – Malware, který sleduje aktivity uživatele bez jeho souhlasu a následně odesílá nasbíraná data tvůrci. (Malware, 2022)
- Ransomware – Typ malware, jehož cílem je uzamknout zařízení anebo zašifrovat data. Poté požaduje od uživatele platbu (výkupné) za přístup k zařízení, nebo dešifrování dat. Tento typ malware se v posledních letech stal pro útočníky velmi oblíbeným, jelikož nabízí možnost rychlého zisku v kryptoměnách. Obrana proti tomuto typu útoků je velmi složitá. Útoky na uživatele sice klesají, nicméně útoky na korporace jsou na vzestupu. Je to dáno i tím, že velké společnosti si mohou dovolit zaplatit větší obnosy a často tak i činí vzhledem k možným finančním ztrátám ze ztracených dat. (Malware, 2022)

II. PRAKTICKÁ ČÁST

4 ANALÝZA BEZPEČNOSTNÍCH FUNKCÍ SOUČASNÝCH WEBOVÝCH PROHLÍŽEČŮ

Volba webového prohlížeče má zásadní vliv na bezpečnost práce s internetem. Některé webové prohlížeče již v základu obsahují bezpečnostní prvky chránící uživatele. Když se nicméně podíváme na statistiku nejpoužívanějších webových prohlížečů, ty úplně nejbezpečnější tam bohužel nenajdeme.

V současnosti dominuje webový prohlížeč Chrome, který využívá prakticky 70 % všech uživatelů internetu. Na druhém místě je prohlížeč Safari s necelými 10 %. Ten je však pouze pro zařízení od společnosti Apple. Na třetím místě je s 8 % prohlížeč Edge, na místě čtvrtém následuje prohlížeč Firefox se 7 %. Zbývající prohlížeče jsou, co se týká počtu uživatelů jen kolem 1 % a méně. (Dean, 2021)



Obr. č. 3 Počet uživatelů desktopových webových prohlížečů (zdroj: https://backlinko.com/browser-market-share)

4.1 Chrome

Nejpoužívanější prohlížeč současnosti poskytuje skvělé uživatelské prostředí a tisíce možných rozšíření. Důvodem je rozsáhlý vývojářský tým, jelikož prohlížeč spadá pod společnost Google. Prohlížeč je tak pravidelně aktualizován a vylepšován. Možné hrozby a zranitelnosti jsou zpravidla řešeny rychleji než u konkurence právě díky rozsáhlému vývojářskému týmu. (Ho, 2022)

Pro prohlížení využívá funkci takzvaného bezpečného prohlížení. Ta se opírá o rozsáhlou databázi nebezpečných stránek, která je k dispozici Googlu jakožto největšímu vyhledávači webových stránek. Tato funkce aktualizována každý den pro vyšší bezpečnost.

To, že prohlížeč spadá pod společnost Google, má na jedné straně pozitivní vliv na bezpečnost prohlížeče vzhledem k možnostem společnosti. Na druhé straně to nicméně přináší rizika pro uživatele. Obchodní model společnosti Google je postaven na sbírání, vytěžování a obchodování s osobními informacemi uživatelů. Tento problém je přítomný i zde u prohlížeče Chrome. Možností pro uživatele, jak zabránit sledování jsou velmi omezené a prohlížeč je taktéž už v základu nastaven na sběr dat o uživatelích. Jedinou možností pro uživatele je spolehnout se na pluginy a na provedení úprav v nastavení prohlížeče. (Ho, 2022)

4.2 Safari

Webový prohlížeč dostupný jen pro zařízení s operačním systémem macOS. V oblasti bezpečnosti uživatele obsahuje velké množství prvků jako: generátor hesel, ochranu uživatele založenou na strojovém učení a soukromý mód, ve kterém je jako výchozí vyhledávač využíván DuckDuckGo. Dalším prvkem zajišťujícím ochranu uživatele je funkce sandbox. Každé okno v prohlížeči je spuštěné ve vlastním sandboxu, což zabraňuje jedné škodlivé stránce poškodit stránky ostatní, nebo samotné zařízení.

I přes použití soukromého módu si ovšem uživatel nemůže být jist tím, že o něm data nebudou zaznamenávána. Společnost Apple, která vlastní prohlížeč Safari již byla přistižena při sbírání dat o uživatelích i v soukromém módu. (Black, 2022)

4.3 Edge

Webový prohlížeč Edge je nástupcem legendárního Internet Exploreru. Prohlížeč obsahuje několik základních bezpečnostních funkcí. Umožňuje blokování vyskakovacích oken a posílání „Do not Track“ požadavků. V jedné z posledních aktualizací, byla do prohlížeče přidána dlouho očekávaná funkce na ochranu před sledováním. (Black, 2022) Edge nabízí 3 základní úrovně zabezpečení. Základní úroveň, vyváženou úroveň a přísnou úroveň. V případě přísné úrovně je blokována většina možností sledování a cookies. Problémem v této přísné úrovni nicméně může být ztráta funkčnosti některých webů, vyžadujících právě cookies pro své fungování. (Ho, 2022)

Důležitým prvkem je taktéž to, že běží v módu sandbox. V tomto módu běží procesy v uzavřeném prostoru a minimalizuje se tak možnost, poškození uživatele infikovanými stránkami.

Nevýhodou tohoto prohlížeče ovšem je nedostatek dalších pluginů, umožňujících uživateli další vylepšení bezpečnosti a ochrany před sledováním. Největší potenciální problém nicméně souvisí s nepravidelností aktualizování. Prohlížeč je aktualizován zpravidla dvakrát ročně. To při rychlém rozvoji nových hrozeb zdaleka nestačí a hrozí tak zneužití zastaralosti. Někteří experti taktéž upozorňují na potenciální riziko plynoucí z uzavřeného zdrojového kódu. Není tak možné ověřit, zda již v něm není zabudována nějaké forma sledování uživatelů. (Black, 2022)

4.4 Firefox

Firefox je jediný opravdu rozšířený prohlížeč postavený na open source platformě. Uživatel zde má tedy jistotu, že kód je pravidelně a nezávisle kontrolován vzhledem k možné přítomnosti bezpečnostních rizik. Za Firefoxem stojí navíc silný vývojářský tým, zajišťující pravidelné aktualizace před novými hrozbami (Black, 2022).

Bezpečnost prohlížeče Firefox pramení primárně z rozsáhlých možností nastavení a možné instalace rozšíření, sloužících pro další zvýšení bezpečnosti uživatele na síti. V základu nicméně bezpečnost není nejlepší a doporučuje se vypnout možnosti jako je telemetrie, která odsílá technická data a taktéž data o uživatelových interakcích na webu. (Sven, 2021) Na druhou stranu je provoz Firefoxu rychlejší než mnohé ostatní prohlížeče. Je to způsobeno automatickou blokací cookies třetích stran. Dále nabízí ochranu před phishingem a malwarem. Nabízí také DNS přes HTTPS (DoH) prohlížení. Toto je důležitý krok pro

ochranu soukromí uživatelů, jelikož u jiných prohlížečů, které tuto funkci nepoužívají dochází při navštívení webové stránky k odeslání žádosti v nezašifrované podobě. V případě využití DoH je tento požadavek zaslán zašifrovaný přes CloudFlare nebo zašifrované servery společnosti NextDNS. Toto zamezuje třetím stranám shromažďovat historii prohlížení daného uživatele. (Ho, 2022)

4.5 Opera

Opera běží na systému Chromium. Obsahuje mnoho bezpečnostních vlastností, které by měly zajistit bezpečnější webové prohlížení. Patří mezi ně ochrana před malwarem, ochrana před podvody, blokování scriptů a zabudovaná VPN služba. Co se týče aktualizací, tak v tomto případě probíhají zhruba jednou za 4–5 týdnů. (Black, 2022)

4.6 Tor prohlížeč

Tor je zkratkou pro „The Onion Router“ projekt zahájený v roce 1995 pro bezpečnou vojenskou komunikaci. Dnes je možné tuto technologii využít i v civilním sektoru. Tor je prohlížeč umožňující přístup na síť, stejně tak i na síť Tor. Prohlížeč je postaven na platformě Mozilly. Do prohlížeče byly přidány extra prvky zajišťující bezpečnost uživatele a jeho anonymitu. V Tor prohlížeči jsou zakázány skripty a všechny stránky jsou převáděny na protokol HTTPS. V základu je prohlížeč nastaven do soukromého módu. Ten po zavření prohlížeče zajistí automatické vymazání aktivity na internetu, cookies a dalších dat. (Jadoon, 2019)

4.7 Brave

Brave je relativně nový webový prohlížeč vytvořený na platformě Chromium s důrazem na bezpečnost uživatelů. Za jeho vznikem stojí Brandon Eich, bývalý zaměstnanec Mozilly. Již v základu bez nutnosti instalace pluginů obsahuje značné množství bezpečnostních prvků. To je užitečné pro uživatele, kteří nehodlají instalovat další bezpečnostní rozšíření, ale chtějí zároveň bezpečný prohlížeč. (Sven, 2021)

V základu obsahuje blokování reklam, manažer hesel, ochranu před sledováním a blokování skriptů. Zároveň prohlížeč automaticky vylepšuje připojení na verzi HTTPS, která je bezpečnější než klasická HTTP. Vzhledem k tomu, že je prohlížeč vytvořen na platformě Chromium, je možné využívat většinu rozšíření pro Chrome, což dále zvyšuje použitelnost.

Brave umožňuje i přístup na síť Tor. V prohlížeči je možné jednoduše otevřít nové okno a přistupovat na web. (Black, 2022)

5 KOMPARACE VYBRANÝCH PROHLÍŽEČŮ A NÁSTROJŮ

Webové prohlížeče jsou vstupní branou uživatele do prostředí internetu. Jeho správný výběr proto hraje zásadní roli, co se týče bezpečnosti a anonymity uživatele na internetu. S ohledem na zadání této práce se zaměřím na vybrané základní bezpečnostní prvky, které zajišťují nejen anonymitu na webu, tedy i minimalizaci digitální stopy, ale také bezpečnost uživatele při použití softwaru.

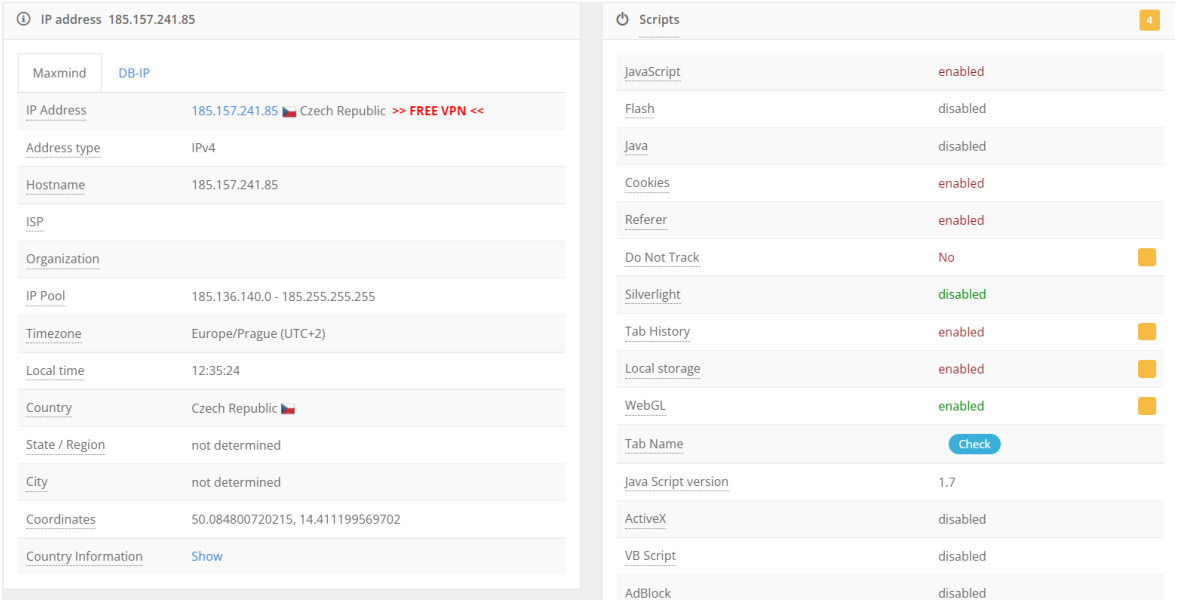
5.1 Anonymní mód prohlížení

I přes využití anonymního módu prohlížeče, je reálná IP adresa a poloha dostupná každé webové stránce, kterou uživatel navštíví. Stejně tak ji vidí i každá reklama. Poskytovatel internetového připojení taktéž vidí a ukládá online aktivity daného uživatele, nehledě na využití anonymního módu prohlížeče.

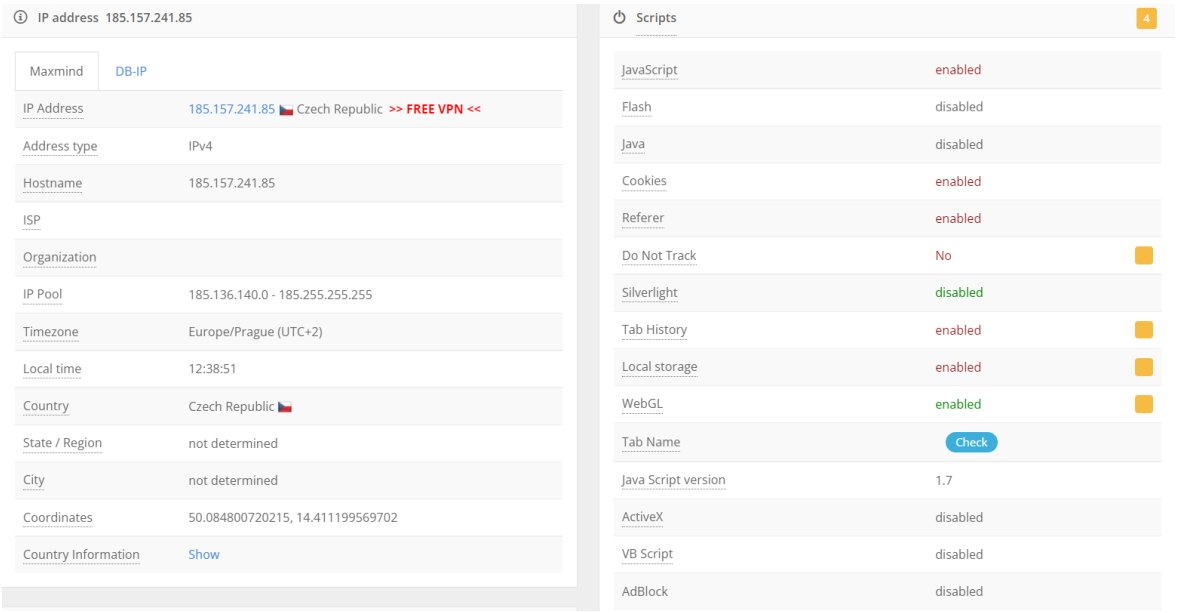
Zde se totiž poskytovatelé internetového připojení musí řídit zákonem č. 127/2005 Sb., o elektronických komunikacích. Ten mimo jiné ukládá i povinnost zaznamenávat a ukládat data uživatelů po dobu šesti měsíců. Přesněji řečeno, jsou to údaje lokalizační a provozní, které jsou vytvářeny nebo zpracovávány (Česká republika, 2015).

Porovnání klasického prohlížení a anonymního módu prohlížeče

Při práci s internetem mohou uživatelé lehce nabýt dojmu, že je jejich pohyb po webu anonymní. Opak je pravdou a toto platí obzvláště v případě využití anonymního módu prohlížení, který nabízí iluzi anonymity a bezpečnosti. Jak je vidět ze srovnání níže, kde byl udělán test na webu (https://ipleak.com/full-report/), rozdíly mezi použitím klasického prohlížení a anonymního módu nejsou.



Obr. č. 4 Bezpečnost při použití klasického módu prohlížení webového prohlížeče Brave (zdroj: vlastní)



Obr. č. 5 Bezpečnost při použití anonymního módu prohlížení webového prohlížeče Brave (zdroj: vlastní)

Z tohoto důvodu se ve srovnání nebudu tímto módem vůbec zaobírat. Jak je totiž vidět na obrázcích výše, v případě použití klasického módu prohlížení bylo dosaženo stejného výsledku, jako při využití prohlížeče v anonymním módu. V obou případech byla viditelná IP adresa zařízení, ze kterého je přistupováno, a i v případě testu skriptů byl výsledek totožný. Zajímavá je například položka „Tab History“ která byla zapnutá i v případě

anonymního prohlížení. Tato funkce umožňuje webové stránce vyslat požadavek na předchozí stránky, ze kterých se uživatel na danou stránku dostal. Takže i přesto, že po vypnutí prohlížeče se historie prohlížení neukládá, v průběhu prohlížení se tato historie dočasně ukládá a pro web je možné vyslat požadavek na tuto informaci.

5.2 Komparace vybraných webových prohlížečů

Webové prohlížeče byly testovány v základním nastavení po instalaci. Cílem bylo totiž zjistit, který prohlížeč je pro uživatel nejbezpečnější pro okamžité používání, bez nutnosti instalace dodatečných pluginů a upravování možností v nastavení. Tyto možnosti umožňují dále zlepšit anonymitu a bezpečnost, nicméně ne každý je využívá, a proto se zde zaměříme na základní nastavení.

Pro následující komparaci bylo vybráno 6 prohlížečů. Chrome, Edge, Firefox a Opera byly vybrány, jako prohlížeče s největším počtem aktivních uživatelů. Prohlížeče Brave a Tor, byly vybrány s ohledem na jejich zaměření na maximální bezpečnost a soukromí uživatele. Tyto prohlížeče byly komparovány v 5 kategoriích rozepsaných níže.

1. Otevřený software – Označuje software, který má svůj zdrojový kód veřejně přístupný. To umožňuje komukoliv ověřit bezpečnost a přítomnost možných bezpečnostních děr. Výsledkem je vyšší bezpečnost a rychlejší náprava nalezených chyb. (What is open source, 2022)
2. Aktualizace – Vzhledem k rychlému rozvoji nových hrozeb, je nutné, aby i software byl co nejčastěji aktualizován. Pravidelnou aktualizací dochází ke zvýšení bezpečnosti uživatele.
3. HTTPS – Značí zkratku pro Hypertext Transfer Protocol Secure. Jedná se o protokol HTTP spolu s protokolem SSL nebo TLS. Tento protokol je využíván pro komunikaci mezi webovým prohlížečem a serverem. Oproti protokolu HTTP nabízí protokol HTTPS bezpečnou šifrovanou komunikaci. (HTTPS, 2022)
4. DOH – Značí zkratku pro DNS over HTTPS. Pro přístup k vybrané webové stránce musí prohlížeč přeložit adresu (například www.google.cz) na IP adresu serveru. Tento požadavek je nicméně standartně vysílán v nezašifrované podobě, a to i v případě využití bezpečného HTTPS spojení. Tento problém řeší vysílání již požadavku na DNS serveru přes HTTPS spojení, kdy i tento první kontakt probíhá již v bezpečné podobě. (Piazza, 2020)

5. Sandbox mód – Z důvodu možnosti obsažení nebezpečného kódu na webových stránkách a možnému ohrožení zařízení a tím i uživatele, jsou v prohlížečích spouštěny buď jednotlivé stránky nebo celý prohlížeč v takzvaném sandbox módu. Tento mód umožňuje ochranu počítače, jelikož vše, co je v něm spuštěno nemá přístup mimo sandbox. Po zavření prohlížeče, nebo stránky dojde k vymazání údajů, včetně možného nebezpečného kódu. (Kumar, 2020)

Tabulka č. 1 – Komparace vybraných webových prohlížečů (zdroj: vlastní)

Prohlížeče	Chrome	Edge	Firefox	Opera	Brave	Tor
Otevřený software	NE	NE	ANO	ANO	ANO	ANO
Aktualizace	ANO	NE	ANO	ANO	ANO	ANO
HTTPS	NE	NE	NE	NE	ANO	ANO
DOH	NE	NE	NE	NE	NE	NE
Sandbox mód	ANO	ANO	ANO	NE	ANO	ANO
Výsledné body	**2**	**1**	**3**	**2**	**4**	**4**

Z výsledků v tabulce výše je zřejmé, že v případě základních bezpečnostních charakteristik vychází nejlépe webový prohlížeč Brave a taktéž prohlížeč Tor. Oba obsahují všechny bezpečnostní prvky až na DOH již v základním nastavení. Naopak nejhůře dopadl prohlížeč Edge, kde bylo nalezených zranitelností nejvíce.

K detailnější komparaci byl následně využit software zaměřený na testování bezpečnosti prohlížeče. Tento nástroj je součástí sbírky testů zaměřených na bezpečnost v online prostoru. Pro potřeby této práce byl použit nástroj na stránce (https://webbrowsertools.com/privacy-test/), zaměřující se na bezpečnost webového prohlížeče. V rámci zmíněného testu bylo všech 6 vybraných prohlížečů otestováno v základním nastavení. Výsledná komparace jejich výsledků je uvedena v tabulce níže.

Komparované parametry u webových prohlížečů:

V případě testu jsou webové prohlížeče posuzovány z hlediska bezpečnosti v 10 parametrech popsaných níže. Tyto parametry byly tvůrci testů vybrány ze zkušeností s oblastí online bezpečnosti. (WebBrowserTools, 2021)

1. WebRTC – Je zkratkou pro „Web Real-Time Communication“ neboli komunikaci webu v reálném čase. Toto je nutné pro video hovory, nebo P2P sdílení (sdílení mezi 2 osobami). I přes to, že je tento problém spojován především s využíváním VPN služeb, je WebRTC leak zranitelnost webových prohlížečů. (Sven, 2021)

2. Cookies – Malý textový soubor uložený v uživatelově zařízení obsahující uživatelské jméno a heslo. Data v cookies jsou vytvořena po spojení se serverem a označena specifickým identifikátorem pro dané zařízení. Server si při každé další návštěvě ze stejného zařízení přečte informace obsažené v cookies. Ty jsou následně využity k identifikaci použitého přístroje, údajů a nastavení. HTTP cookies můžeme rozdělit podle vlastností na jednorázové a trvalé cookies.
3. Pluginy – Jelikož není možné vyhodnotit, jestli nainstalované pluginy jsou pro uživatele bezpečné nebo ne, je v případě, kdy je pro uživatele důležitá anonymita a bezpečnost doporučeno nemít žádné pluginy nainstalované. (Browser Privacy Test, 2021)
4. Do Not Track – Umožňuje prohlížeči zakázat webové stránce sledování aktivit uživatele skrze analytické nástroje. (Browser Privacy Test, 2021)
5. Sledování hypertextového odkazu – Schopnost prohlížeče blokovat odesílání údajů o uživatelově interakci s odkazy na webu. (Browser Privacy Test, 2021)
6. Povolený Javascript – Javascript je nutný pro správné fungování některých webů, nicméně pro bezpečnější užívání internetu je doporučené ho mít vypnutý. A to vzhledem k možnosti spuštění škodlivého scriptu. (Browser Privacy Test, 2021)
7. Povolený Flash – S ohledem na bezpečnost je doporučené mít zablokované použití schopnosti flash. Jeho využívání je spojené s bezpečnostními hrozbami. (Browser Privacy Test, 2021)
8. Přístup k poloze zařízení – možná zranitelnost
9. Přístup k mikrofonu – možná zranitelnost
10. Přístup ke kameře – možná zranitelnost

Tabulka č. 2 – Porovnání vybraných zranitelností u webových prohlížečů (zdroj: vlastní)

Zranitelnosti	Chrome	Edge	Firefox	Opera	Brave	Tor
WebRTC	ANO	ANO	NE	ANO	ANO	NE
Cookies	ANO	ANO	ANO	ANO	ANO	NE
Pluginy	ANO	ANO	ANO	ANO	ANO	NE
DoNotTrack	ANO	ANO	NE	ANO	ANO	NE
Sledování Hypertextového odkazu	NE	NE	NE	NE	NE	NE
Povolený JavaScript	ANO	ANO	ANO	ANO	ANO	NE
Povolený Flash	NE	NE	NE	NE	NE	NE
Přístup k poloze zařízení	NE	NE	NE	NE	NE	NE
Přístup k mikrofonu	NE	NE	NE	NE	NE	NE
Přístup ke kameře	NE	NE	NE	NE	NE	NE
Výsledné body	**5**	**5**	**7**	**5**	**5**	**10**

Při detailnější analýze možných zranitelností je zřejmé, že nejbezpečnějším prohlížečem je prohlížeč Tor. Ten je vytvořen s ohledem na maximální anonymitu uživatele, takže tento výsledek není překvapením. Nicméně je nutné si zde uvědomit, že tento prohlížeč není ideální pro každodenní užívání internetu. Z důvodu dosažení maximální bezpečnosti je funkčnost některých webů silně omezena. Taktéž použití tohoto prohlížeče je spojeno s využitím sítě Tor. Tato síť vzhledem k tomu, jak je navržena, není dostatečně rychlá pro každodenní použití.

Jako nejbezpečnější prohlížeč pro každodenní použití se tedy jeví prohlížeč Firefox. U něj byly nalezeny zranitelnosti jen u tří zkoumaných prvků. U zbývajích prohlížečů bylo nalezeno shodně 5 zranitelností. Je zajímavé, že všechny tyto zranitelnosti jsou ve stejných bodech testování – problém s WebRTC, Cookies, Pluginy, DoNotTrack a problém s povoleným JavaScriptem.

Tabulka č. 3 – Výsledné zhodnocení webových prohlížečů (zdroj: vlastní)

Prohlížeče	Chrome	Edge	Firefox	Opera	Brave	Tor
Výsledek	**7/15**	**6/15**	**10/15**	**7/15**	**9/15**	**14/15**

Z výsledného hodnocení je patrné, že nejbezpečnějším, nejvíce anonymním prohlížečem a tedy i prohlížečem zanechávajícím nejmenší digitální stopu uživatele je prohlížeč TOR. Ten dosáhl v hodnocení 14 bodů z 15 možných. Nicméně o jeho limitacích, co se týkají praktičnosti jsem již hovořil výše. Pro každodenní použití je tedy nutné podívat se na druhé a třetí místo. Na druhém místě se umístil prohlížeč Firefox s 10 body a o bod za ním, na místě třetím prohlížeč Brave. Oba tyto prohlížeče jsou vyvíjeny s ohledem

na maximální anonymitu a bezpečnost uživatelů, takže jejich umístění zde není překvapením. Oba prohlížeče obsahují zranitelnosti, nicméně v porovnání se zbytkem jsou na tom dobře. Nejpoužívanější prohlížeče, tedy Chrome a Edge, jsou na tom z hlediska bezpečnosti uživatele výrazně hůře. Kdy prohlížeč Chrome dosáhl ve výsledku jen na 7 bodů z 15 a prohlížeč Edge dokonce jen na 6 bodů. V těchto případech bylo nalezených zranitelností hodně.

5.3 Nástroje na zabránění sledovacích aktivit v prohlížečích

Některé nedostatečnosti webových prohlížečů v oblasti bezpečnosti uživatele se dají vyřešit instalací specializovaných nástrojů. Pro potřeby této práce se zaměřím na tři populární nástroje pro blokaci sledování uživatele při užívání internetu. Tyto nástroje jsou volně dostupné pro celou řadu prohlížečů. V případě této práce, byly instalovány do prohlížeče Firefox, který, jak je zřejmé z předchozí kapitoly, patří mezi bezpečnější prohlížeče.

Nabídka nástrojů se zaměřením na blokaci sledování uživatelů je pestrá. Pro účely této práce byly vybrány nástroje, které jsou podle počtu uživatelů nejužívanější.

5.3.1 DuckDuckGo Privacy Esential

- Autor: DuckDuckGo
- Verze: 2022.3.30
- Poslední aktualizace: 8.4.2022

Společnost DuckDuckGo stojí i za stejnojmeným vyhledávačem, který na rozdíl od například nejvyužívanějšího vyhledávače Google o uživatelích nesbírá data o vyhledávání. Tento nástroj blokuje skryté trackery a vynucuje si u webů použití šifrovaného spojení.

5.3.2 Ghostery

- Autor: Ghostery
- Verze: 8.6.2
- Poslední aktualizace: 10.4.2022

Nástroj Ghostery je primárně určený pro blokování reklamy a taktéž pro blokování trackerů. Automatická blokace reklamy má za výsledek nejen vyšší anonymitu uživatele, ale taktéž rychlejší načítání webových stránek. Nástroj taktéž umožnuje zobrazení detailních informací a možnost přizpůsobit si nastavení podle preferencí uživatele.

5.3.3 Privacy Badger

- Autor: EFF Technologists
- Verze: 2021.11.23.1
- Poslední aktualizace: 6.12.2021

Nástroj Privacy Badger se učí při užívání automaticky blokovat prvky pro sledování uživatelů v závislosti na jejich chování. Zároveň vysílá požadavek Do Not Track a automaticky nahrazuje užitečné, ale potenciálně nebezpečné prvky (například přehrávače videa) pomocí prvků, aktivovaných kliknutím. Tím se zamezí automatickému sběru dat, ale zároveň to umožňuje bezproblémové užití webu.

5.4 Komparace vybraných nástrojů

Ze srovnání deseti nejnavštěvovanějších stránek v České republice níže lze vyčíst, že až na výjimky se na každé stránce nachází prvky sledující pohyb a aktivity uživatele. Jediné výjimky, kdy žádný ze zkoumaných softwarů nenalezl sledovací prvky, byly webové stránky wikipedia.org a facebook.com. V případě stránky facebook.com je nutné si ovšem uvědomit na čem je postaven jejich obchodní model. Absence sledovacích prvků třetích stran na jejich webu je vykoupena tím, že společnost Facebook sama o uživateli sbírá všechny dostupné informace.

Tabulka č. 4 – Porovnání vybraných nástrojů (zdroj: vlastní)

	DuckDuckGo Privacy Esential	Ghostery	Privacy Badger
google.com	0	2	0
seznam.cz	5	5	7
youtube.com	0	4	2
facebook.com	0	0	0
novinky.cz	2	4	6
idnes.cz	7	6	6
stream.cz	2	3	1
super.cz	7	5	7
wikipedia.org	0	0	0
sport.cz	13	19	11
Výsledek	**36**	**48**	**40**

U všech ostatních webů byl alespoň jedním nástrojem zaznamenán sledovací prvek. Jejich nejvyšší množství bylo zaznamenáno v případě zpravodajských webů. Především na webech

idnes.cz, super.cz a sport.cz. Na webu sport.cz bylo v případě nástroje Ghostery zaznamenáno dokonce 19 aktivních sledovacích prvků.

Při celkovém srovnání těchto nástrojů je patrný rozdíl v úspěšnosti blokování sledovacích prvků. Nejvyšší účinnost celkově zaznamenal nástroj Ghostery, který na deseti webových stránkách nalezl a částečně zablokoval 48 sledovacích prvků. V některých případech jako například u webu super.cz byl méně úspěšný než ostatní nástroje. Nástroje tohoto typu umožnují uživateli snížit svou digitální stopu, kdy nejlepšího výsledku dosáhl nástroj Ghostery.

5.5 IP (Internet Protocol) adresa

IP adresa je číslo identifikující síťové rozhraní v síti. Díky ní je možné identifikovat individuálního uživatele. To je důležité pro přenos souborů, příjem emailů a podobně. IP adresy můžeme rozdělit na dvě kategorie: statické a dynamické. V případě statických adres je jejich adresa neměnná. V případě dynamických se adresa mění v závislosti na konkrétním připojení. Díky připojení k jinému routeru nebo například k jiné wifi síti se nám změní i naše IP adresa. (Chivers, 2021)

V současnosti se využívají dvě verze internetového protokolu. IPv4 a IPv6. IPv4 je starší systém, využívající 4 osmibitová pole oddělená tečkou. Standartní zápis vypadá například takto (135.139.073.054). Počítač nicméně pracuje ve dvojkové soustavě a v té toto samé číslo vypadá jako (10000111.10001011.01001001.00110110). Maximální číslo je tedy 255, které je v binární soustavě zaznamenáno jako 11111111. Z tohoto vychází i omezení počtu možných adres, kdy každá musí být specifická, aby nedošlo k záměně. Počet adres je omezen na zhruba 4,3 miliardy. Nicméně ne všechny adresy mohou být využity, jelikož některé jsou rezervovány pro potřeby protokolu. I přesto tento počet, ač se zdá dostatečný, už dnes při rapidním rozvoji technologií dávno nestačí. (Brooks, 2018)

Byla proto zavedena nová verze a to IPv6. Jejím hlavním cílem bylo vyřešit problém s nedostatkem adres, jako tomu hrozilo u IPv4. Tento nový protokol proto nepracuje s 32bity, ale byl rozšířen na 128 bitů. To umožnilo nárůst možných adres na $3{,}4 \times 10^{38}$. (Brooks, 2018)

Problémem může být zneužití informací získaných z naší IP adresy. Není z ní možné získat přesnou adresu s ulicí a číslem popisným, nicméně je možné určit přibližnou polohu. Například město, nebo jeho část. I proto se dynamická IP adresa uživatele mění s tím, jak

se připojuje k jiným sítím. Většinou není zjištěna IP adresa samotného zařízení, ale IP adresa routeru, přes které je zařízení k internetu připojeno. Přesněji řečeno je určena geografická pozice nejbližšího serveru poskytovatele internetového připojení a jeho název. (Chivers, 2021)

Možnosti zneužití zde jsou možná ze strany účastníků:

- Bezpečnostní složky – Mohou využívat a skládat dohromady informace o osobách a sledovat, zda se neúčastní nelegálních činností.
- Zaměstnavatelé – Mohou sledovat, jak zaměstnanci tráví svůj čas v práci, popřípadě i kde a jaké weby navštěvují.
- Obchodníci – Mohou zjišťovat polohu ke zjištění jaké služby a produkty nabídnout, nebo mohou porovnávat polohu s platební metodou a adresou doručení, kvůli možnosti odhalit podvodníky.
- Předplacené služby – Služby typu Netflix využívají zjišťování polohy podle IP adresy k blokaci určitých služeb a obsahu.
- Chatovací aplikace a fóra – Mohou využít IP adresu k blokaci uživatelů. (Chivers, 2021)

IP Address	185.157.241.85
ASN	39235
City	Borsice
State/Region	Zlinsky kraj
Country Code	Czechia
Postal Code	687 09
ISP	Nordic Telecom Regional s.r.o.
Time Zone	+01:00

IP2Location.com Results

IP Address	185.157.241.85
ASN	39235
City	Kostelany nad Moravou
State/Region	Zlín
Country Code	CZ
Postal Code	686 01
ISP	Nordic Telecom Regional s.r.o.
Time Zone	Europe/Prague

ipdata.co Results

Obr. č. 6 Ukázka zjištění polohy z IP adresy
(zdroj vlastní – dostupné z: IP Address Lookup – IP Lookup Tool, 2022)

Jak je možné vidět na obrázku výše, zjištění přibližné polohy je velmi snadné. Je ovšem vidět, že poloha je jen přibližná. V obou případech byl shodně určen jako poskytovatel internetového připojení Nordic Telecom Regional s.r.o. V prvním případě byla dle IP adresy určena poloha v obci Boršice s poštovním směrovacím číslem 687 09. Nepřesnost je tedy několik kilometrů vzhledem k reálné poloze na fakultní adrese na Studentském náměstí v Uherském Hradišti. V druhém případě byla jako adresa ukázána obec Kostelany nad Moravou ležící taktéž pár kilometrů od Uherského Hradiště. Zde vzhledem ke shodě poštovního směrovacího čísla 686 01, které je shodné jak pro Kostelany nad Moravou, tak i pro část Uherského Hradiště – přesněji i pro část kde sídlí fakulta, mohlo dojít k záměně.

6 SKRYTÍ FYZICKÉ ADRESY POČÍTAČE

I přes využití bezpečného webového prohlížeče a instalace vybraného nástroje je reálná IP adresa uživatele viditelná. Možností, jak tento problém vyřešit je hned několik.

6.1 Proxy server

Proxy servery souvisí s kontrolou síťové komunikace. Umožňují kontrolovat obsah dat, ke kterým budou uživatelé přistupovat včetně jejich obsahu. V případě této práce primárně hovoříme o takzvané web proxy.

Nicméně rozlišovány jsou tři základní typy:

- Reverzní proxy server – Tento typ proxy serveru bývá zpravidla nasazován před webovým serverem. Jeho úkolem je zpracovat požadavky klientů buď samostatně, nebo tyto požadavky předat dalším serverům. Výhodou je možnost řídit tuto selekci dle například klientem požadované URL, nebo umožňuje balancování zátěže jednotlivých serverů, provádění komprese dat a akceleraci šifrování. (Kolouch, Bašta, 2019)
- Forward Proxy server – Umožňuje řídit přístup konkrétních uživatelů k cílovému serveru (webovým stránkám). Stejně tak je možné určit rozsah přístupu k webovým stránkám pro konkrétní uživatele. Funkce tohoto serveru může být spojena i s dalším bezpečnostním prvkem, jako je antivirus, s jehož pomocí je možné kontrolovat přenášená data a popřípadě tato data i zablokovat. (Kolouch, Bašta, 2019)
- Open proxy server – Tento typ proxy serveru je dostupný každému uživateli na internetu. Některé jsou přístupné jednoduše na jejich webových stránkách, jiné je nutné napřed nakonfigurovat. Jejich výhodou je navíc existence seznamů open proxy serverů, ze kterých si uživatel může vybrat podle jejich fyzického umístění. Například v případě nutnosti přistupovat na server, jehož obsah je přístupný jen v určitých zemích. Použití tohoto typu serveru s sebou nese i bezpečnostní rizika. Nemusí být totiž známé, kdo daný proxy server vlastní a má ho pod kontrolou, nebo zda do webových stránek nebyl přidán škodlivý obsah. (Kolouch, Bašta, 2019)

6.2 TOR prohlížeč

V roce 1995 zahájila laboratoř amerického námořnictva projekt na vývoj anonymní sítě pro vojenskou komunikaci. Název projektu byl Onion Router. Výsledkem byla síť s nízkou

latencí využívající vrstvu šifrování pro anonymitu. Následně byla tato síť vylepšena. Tato druhá generace byla pojmenována The Onion Router (TOR). Hlavním cílem projektu bylo oddělit identifikační údaje z přenosu a vyvinutí anonymní komunikační sítě pro vojenskou komunikaci. (Jadoon, 2019)

Síť TOR se skládá z celosvětové sítě relé (přenašečů), které pomáhají v dosažení soukromí a anonymity pro uživatele internetu. Pro každou komunikaci Tor síť vytvoří virtuální okruh, skládající se alespoň ze tří po sobě jdoucích, náhodně vybraných relé. Informace ohledně těchto relé je stažena klientem Tor na zařízení z řídícího serveru. Dle posledních údajů je dnes více než 2.5 milionu aktivních Tor uživatelů a více než 6000 relé k přenosu dat, poskytující propustnost sítě 25.5 Gbs. (Jadoon, 2019)

Šifrovací klíče jsou vyměňovány s vybranými relé za použití Diffie-Hellmanova protokolu na výměnu klíčů. V počátečním bodě jsou datové balíčky zašifrovány několikrát. Pro každé relé, kterým bude datový baliček procházet je zvoleno vlastní šifrování. To znamená, že pro první relé je určena vnější vrstva šifrování a poslední relé určené pro výstup dešifruje poslední vrstvu šifrování. Soukromí dat je tak zajištěno až po poslední předání. V případě použití https přes síť tor, jsou i tato data předávána posledním relé šifrována. Prohlížeč Tor je navíc nastaven tak, aby každých 10 minut měnil cestu, přes kterou dané datové balíčky budou putovat. Toto dále zvyšuje anonymitu při použití. (Jadoon, 2019)

K zajištění proti možným úrokům je síť nastavena tak, aby došlo k přímému spojení s nejbližším „sourozencem“. To zajištuje nemožnost pozměnění informací. První relé se následně spojí s dalším sourozencem, tak aby došlo k dokončení vybraného řetězce. Kvůli možnostem útoků typu man-in-the-middle je toto spojení vynucené. Každé relé je tak schopné zahájit spojení jen s předem určeným sourozencem a s nikým jiným. (Forte, 2006)

6.3 Tails

Tails je zkratkou pro „The Amnesic Incognito Live Systém“. Systém je postaven na linuxové distribuci Debian. Funkcemi je podobný předchozí verzi „Incognito“ postavené na linuxové verzi Gentoo. Tails je určen jako samostatný operační systém spouštěný z DVD, nebo z flash disku nastaveného pouze pro čtení a nikoliv zápis.

Tím, že je systém spouštěn pouze z média určeného pro čtení a na hard disk se neukládají záznamy o jeho používání, umožňuje vyšší úroveň bezpečnosti. Samotné zařízení tedy

při možné prohlídce neposkytne vyšetřovatelům žádné užitečné informace a ti se tak budou muset zaměřit na zanechaná data na síti.

Součástí operačního systému je i množství předinstalovaných aplikací speciálně vybraných pro zajištění anonymity uživatele. Jako internetový prohlížeč zde najdeme prohlížeč Tor, pro šifrovanou komunikaci nástroj Pidgin a na emaily je zde předinstalovaný program Claws s šifrováním. Přístup k „dark netu“ je zajišťován pomocí Onion routingu (Tor) nebo pomocí „the Invisible Internet Project“ (I2P). (Abraham, 2016)

6.4 Virtuální privátní síť

VPN je zkratkou pro virtuální privátní síť. Z bezpečnostních důvodů organizace naráží na problém se zabezpečením svých služeb online. Na jedné straně mají potřebu chránit svá data a na straně druhé mají potřebu se k datům uložených na svých serverech připojit odkudkoli. Obzvláště v posledních letech, kdy mnohé organizace přecházely z důvodu pandemie na home-office. Stejný problém nicméně byl v korporátním prostředí řešen i dříve s ohledem na dislokaci svých poboček, ale se zachováním připojení na svůj server. Pro tyto účely začaly organizace využívat služeb VPN sítí. Možnost využití se nicméně neomezuje jen na korporátní prostředí, ale i na soukromou sféru. (Kolouch a Bašta, 2019)

Starší verze VPN byly postaveny na protokolu MS-CHAP-v2. Dnes je tento protokol považován za zastaralý, s několika závažnými slabinami. Protokol je založený na „Challenge Handshake Authentication Protocol“ (CHAP). To ovšem znamená, nutnost protokolu mít uživatelská hesla uložená v čitelné podobě. Toto přestavuje bezpečnostní riziko a dnes se již tento přístup nevyužívá. Momentálně se nejčastěji využívá open source řešení „OpenVPN server“. Ten nabízí množství autentizačních protokolů. V případě certifikátů se využívá RSA s délkou klíče alespoň 4096 bitů. Tento certifikát se využívá pro autentizaci. Pro samotné šifrování dat je využito 256bitového AES-CBC. Nicméně využití OpenVPN má i značnou nevýhodu. Je jí potřeba kvalitně vygenerovaného soukromého a veřejného klíče. Dále je nutné zažádat o vydání certifikátu a ten doručit na certifikační autoritu. Na ní je nutné certifikát podepsat a tento podepsaný certifikát zpět doručit uživateli. (Kolouch a Bašta, 2019)

6.4.1 Princip fungování virtuální privátní sítě

Virtuální privátní sít funguje na principu vytvoření bezpečného připojení mezi vzdálenými zařízeními, nebo vzdáleným zařízením a sítí. Samotné spojení je zabezpečeno šifrováním, dostupným jen pro oba koncové prvky.

K lepšímu pochopení principu VPN služby je nutné si uvědomit princip, jakým je nám umožněn přístup k webovým stránkám. Každé zařízení připojené k internetu má svou IP adresu, která slouží k jeho identifikaci. Pokud vyšleme požadavek na spojení s webovou stránkou například www.utb.cz, je tato žádost z našeho prohlížeče vyslána na server UTB. Po spojení tato žádost vytvoří komunikační kanál pro spojení se serverem, přes který jsou nám poskytnuty požadované informace. Tato cesta ovšem není přímá. V závislosti na poloze serveru a poloze uživatele, vysílajícího požadavek je cesta ustanovena přes další sítě nebo uzly. (Ramirez, 2020)

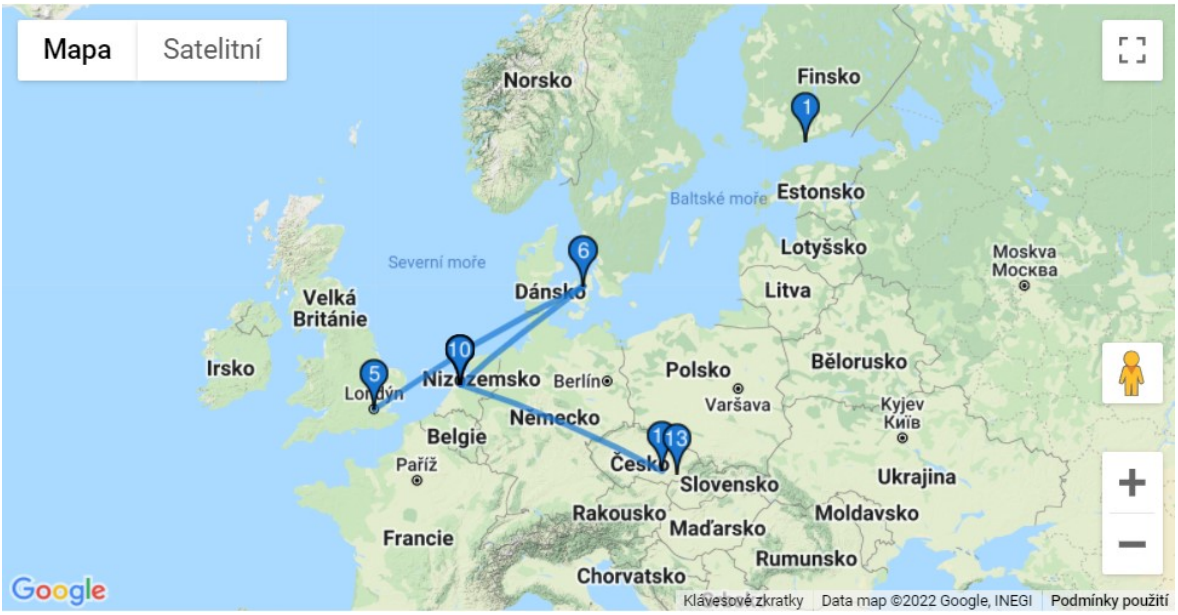
Jak je vidět na obrázcích níže, v případě přístupu na webové stránky UTB s IP adresou (195.178.88.109) za použití softwaru „traceroute“. Který je přístupný na webových stránkách (https://gsuite.tools/traceroute), vede cesta z jejich serveru (94.237.52.1) nacházejícím se ve Finsku na stránky UTB přes 12 dalších adres. To může být problém, jelikož každá adresa, přes kterou data prochází může být nastavena pro sbírání informací. Obzvláště v případě využití HTTP, kdy je tento požadavek posílán v podobě nezašifrovaného textu.

traceroute to www.utb.cz (**195.178.88.109**), 30 hops max

Hop	Host	IP	Time (ms)
1	_gateway	94.237.52.1	0.122ms
2	100.69.38.161	100.69.38.161	0.252ms
3	172.17.255.213	172.17.255.213	0.346ms
4	172.17.255.249	172.17.255.249	0.209ms
5	195.66.225.24	195.66.225.24	0.816ms
6	ndn-gw.mx1.lon.uk.geant.net	109.105.102.98	15.104ms
7	ae9.mx1.ams.nl.geant.net	62.40.98.128	21.427ms
8	ae7.mx1.fra.de.geant.net	62.40.98.187	21.650ms
9	ae8.mx1.pra.cz.geant.net	62.40.98.193	26.501ms
10	cesnet-ias-cesnet-gw.pra.cz.geant.net	83.97.88.42	25.542ms
11	195.113.157.167	195.113.157.167	25.728ms
12	*	*	*
13	www.utb.cz	195.178.88.109	25.800ms

Obr. č. 7 Přístup ze serveru ve Finsku na stránky UTB

(zdroj: vlastní dostupné z: Visual Traceroute, 2021)



Obr. č. 8 – Přístup ze serveru ve Finsku na stránky UTB – mapa
(zdroj: vlastní dostupné z: Visual Traceroute, 2021)

Tento problém se mimo jiné snaží vyřešit právě VPN. Ta vytvoří šifrovaný tunel, mezi uživatelem a serverem. To zabrání možnému sledování třetích stran po cestě, jelikož data jsou pro ně nečitelná. V závislosti na použité VPN službě je možné si cílový server zvolit i v jiné zemi, než se uživatel nachází. To je vhodné například při obcházení geoblokací. (Ramirez, 2020)

6.4.2 Základní typy virtuální privátní sítě

- SSL VPN (Secure Sockets Layers VPN) – VPN technologie založená na HTTPS protokolu. Pracuje mezi vrstvou 4 (transportní vrstva) a vrstvou 7 (aplikační vrstva) na modelu OSI (Open Systems Interconection). Pro navázání bezpečného spojení využívá SSL VPN ověření založené na certifikátech. Dále šifrování dat a ověřovací mechanismus pro celistvost zpráv poskytnutý SSL protokolem. Použití tohoto typu VPN je převážně ve webovém vzdáleném bezpečném přístupu. Zajišťuje ale i pro uživatele bezpečné připojení do vnitřní sítě společnosti. (Zhipeng, 2018)
- IPSec VPN (internet Protocol Security VPN) – Základem je protokol IPSec, který poskytuje takzvanou tunelovou bezpečnost. IPSec využívá end-to-end přístup vyvinutý Komisí pro technickou stránku internetu (IETF). Využívá IP komunikaci spolu s šifrováním informací k zajištění bezpečnosti dat posílaných po síti. (Zhipeng, 2018)

- MPLS VPN (Multiprotocol Label Switching VPN) – Je typem IPSec VPN založené na technologie MPLS. Největší výhodou tohoto typu VPN je využití kombinace technologií pro routing a switching, které vycházejí z vrstev 2 a 3 technologie OSI. I proto je stále častěji preferována operátory při zajišťování spojení ve společnostech. (Zhipeng, 2018)

6.4.3 Decentralizovaná virtuální privátní síť

Při použití služby VPN je uživatel odkázán na společnost poskytující danou službu. To s sebou přináší nicméně i rizika. Uživateli nezbývá nic jiného než věřit dané společnosti, že neukládá žádné logy, ani nezasahuje do jeho připojení. Tyto společnosti se navíc pro své fungování mnohdy spoléhají na cloudová úložiště pro umožnění připojení po celém světě. To přináší možná bezpečnostní rizika, která mohou umožnit sledování uživatele. (Varvello, 2021)

S ohledem na výše uvedené hrozby vnikla decentralizovaná virtuální privátní síť (dVPN). Jedná se o nový trend, nicméně dnes už se jedná o miliony aktivních denních uživatelů. V případě použití sítě dVPN jsou uživatelé jak klienti, tak i poskytovatelé. Síť funguje na principu Peer-to-Peer (P2P). Pro nezkušené uživatele to nicméně přináší rizika. Vzhledem k principu, na jakém síť funguje nemohou uživatelé vyloučit, že přes jejich zařízení nebude šířen nelegální obsah. Stejně tak je zde i možnost zneužití uživatelů jako výstupních bodů v síti pro provádění DDoS útoků. (Varvello, 2021)

6.5 Ukládání dat o uživatelích

Hlavní funkcí VPN služby je anonymizace uživatele při používání internetu. Z tohoto důvodu je důležité se při výběru VPN služby zaměřit i na to, zda dodržuje takzvanou „No Log Policy“. Ta uživateli garantuje, že společnost a servery na kterých služba běží o něm neshromažďuje žádné informace, které by mohly být použity pro identifikaci jeho online aktivit. I když je společností poskytující VPN službu tato „No Log Policy“ garantována, je nutné si ji ověřit. Ne každá společnost tyto zásady zcela dodržuje a určitá data o uživatelích prodává. Ne vždy je nedodržení „No Log Policy“ způsobené snahou společnosti o monetizaci dat uživatele. Většina států nařizuje internetovým poskytovatelům shromažďovat základní informace o uživatelích, a i společnosti provozující VPN službu se jimi musí řídit. Je nutné si proto při výběru VPN služby ověřit, že sídlí v zemi, kde toto neplatí. (Johnson, 2022)

6.6 Komparace vybraných virtuálních privátních sítí

Z nástrojů vhodných pro skrytí reálné IP adresy se s ohledem na použitelnost a míru bezpečnosti pro uživatele jeví jako nejlepší volba VPN služba. Proto i pro účely této práce byly porovnávány vybrané VPN služby s ohledem na funkčnost a úroveň anonymity, kterou poskytují. Jako podklady ke srovnání bylo vycházeno z rozsáhlé práce Roba Mardisala z roku 2021, kde porovnával 78 nejpoužívanějších VPN služeb (Mardisal, 2021).
Pro srovnání bylo vybráno 11 VPN služeb s ohledem na dostupnost pro uživatele. Vybráno bylo 5 VPN služeb (NordVPN, SurfShark, ExpressVPN, Perfect-Privacy, Ip-Vanish a Proton VPN) jakožto služby s největším počtem uživatelů. V druhé kategorii byly vybrány VPN služby společné s antivirovými programy (Avast Secureline, AVG VPN, Norton Wifi Privacy a Kaspersky VPN). V tomto případě byla brána v potaz jednoduchost aktivace a dostupnost pro uživatele, jelikož antivirový program se nachází prakticky na každém zařízení. Jako poslední byla hodnocena Opera VPN nacházející se jako součást webového prohlížeče Opera. Tento zástupce byl vybrán pro možnost aktivovat si VPN službu bez nutnosti instalace dalšího software a taktéž proto, že služba je na rozdíl od ostatních porovnávaných VPN zdarma.

6.6.1 Komparace základních parametrů

V první části byly porovnány základní parametry s ohledem na funkčnost VPN služby. Vybráno bylo 6 parametrů, jeden nicméně jen jako informační a nebyl hodnocen. Parametry byly vybrány na základně rozsáhlé práce Roba Mardisala. V té porovnává z hlediska bezpečnosti 78 nejpoužívanějších VPN alužeb. (Mardisal, 2021)

1. Sídlo společnosti – S ohledem na dodržování No Log Policy popsané v kapitole 6.5 byla v tabulce uvedena sídla společností. Tento bod ovšem nebyl hodnocen.
2. Spolupráce – Souvisí s bodem č. 1. Zde je hodnocena ochota společností spolupráce s bezpečnostními složkami. Pro anonymitu uživatele je nutné, aby služba nesdílela žádné informace o jeho aktivitách.
3. Rychlost – Pro použitelnost je nutné, aby uživatel nebyl omezován rychlostí služby.
4. Servery/Státy – Větší množství serverů rozmístěných po celém světě je důležitým prvkem pro rychlost služby. Vyšší počet serverů je taktéž méně náchylný na možné omezení služby.

5. Počet zařízení – Zde je hodnocen počet zařízení, která si může uživatel ke službě naráz připojit. V dnešní době, kdy je běžné mít u sebe počítač, telefon a mnohdy i tablet zároveň je nutné chránit všechna zařízení současně. Proto je zde hodnoceno i množství zařízení, které je možné naráz připojit.
6. Torrent – Zde je hodnocena možnost použití služby typu P2P přes VPN službu. Pro mnohé uživatele by absence této možnosti mohla znamenat komplikace.

Tabulka č. 5 – Komparace základních parametrů VPN služeb (zdroj: vlastní dostupné z: Mardisal, 2021)

	Sídlo společnosti	Spolupráce	Rychlost	Servery/Státy	Počet zařízení	Torrent
NordVPN	Panama	NE	Rychlá	5430/60	6	ANO
SurfShark	Britské Panenské o.	NE	Rychlá	800/50	Neomezeně	ANO
ExpressVPN	Britské Panenské o.	NE	Rychlá	3000/93	3	ANO
Perfect-Privacy	Švýcarsko	Spolupráce	Průměrná	55/24	Neomezeně	ANO
IP-Vanish	USA	Úplná spolupráce	Rychlá	1200/60	10	Omezeně
Avast Secureline	Česká republika	Spolupráce	Rychlá	52/34	5	Omezeně
Proton VPN	Švýcarsko	Spolupráce	Průměrná	345/32	10	Omezeně
AVG VPN	Česká republika	NE	Pomalá	50/36	1	Omezeně
Norton Wifi Privacy	USA	Úplná spolupráce	Rychlá	30/23	10	NE
Kaspersky VPN	Rusko	NE	Průměrná	2000/30	5	NE
Opera VPN	Norsko	Úplná spolupráce	Pomalá	10/5	Zdarma	NE

6.6.2 Komparace bezpečnostních aspektů

V druhé části srovnání byly porovnávány vlastnosti s ohledem na bezpečnost a zachování anonymity uživatele. Zde bylo posuzováno 6 bodů, kdy při jejich výběru bylo vycházeno z práce Roba Mardisala: (Mardisal, 2021)

1. IP Leak – Únik reálné IP adresy i přes použití VPN služby. Jedná se o bezpečnostní riziko, jelikož každá navštívená stránka a i poskytovatel internetového připojení může sledovat online aktivity uživatele.
2. WebRTC Leak – WebRTC je zkratkou pro Web Real-Time Communication. Jedná se o technologii webových prohlížečů umožňující video hovory, volání a P2P sdílení. Problémem zde je, že při této komunikaci dochází k výměně reálné IP adrese uživatele.

3. DNS Leak – DNS je zkratkou pro (Domain Name Systém) jedná se o decentralizovaný systém doménových jmen. Před připojením k webové stránce dochází prvně ke kontaktu DNS serveru, který si vyžádá IP adresu dané stránky. Tento proces nicméně probíhá v nezašifrované podobě. VPN služba by měla tyto spojení šifrovat, aby zde nedocházelo k úniku reálné IP adresy uživatele.
4. Zranitelnost – Zde byly testovány možné zranitelnosti například s ohledem na nainstalované nástroje v prohlížeči.
5. Ukládání logů – Pro zajištění anonymity uživatele nesmí VPN služba ukládat žádné informace o jeho online aktivitách.
6. Automatické odpojení – Důležitý prvek pro bezpečnost a anonymitu uživatele VPN služby. Jedná se o prvek, který zajistí automatické odpojení od internetu, pokud je zjištěno, že VPN služba není aktivní, nebo přestala fungovat. Zajišťuje, že ani v případě výpadku funkčnosti VPN služby nedojde k úniku reálné IP adresy uživatele.

Tabulka č. 6 - Komparace bezpečnostních parametrů VPN služeb (zdroj: vlastní dostupné z: Mardisal, 2021)

	Únik IP	Únik WebRTC	Únik DNS	Zranitelnosti	Ukládání logů	Automatické odpojení
NordVPN	NE	NE	NE	NE	NE	ANO
SurfShark	NE	NE	NE	NE	NE	ANO
ExpressVPN	NE	NE	NE	NE	NE	ANO
Perfect-Privacy	NE	NE	NE	NE	NE	ANO
IP-Vanish	NE	NE	NE	NE	NE	ANO
Avast Secureline	NE	NE	NE	NE	NE	ANO
Proton VPN	NE	NE	NE	NE	NE	ANO
AVG VPN	NE	NE	NE	NE	ANO	ANO
Norton Wifi Privacy	NE	NE	NE	NE	ANO	NE
Kaspersky VPN	NE	NE	NE	NE	ANO	NE
Opera VPN	NE	NE	NE	ANO	ANO	NE

Z výsledné tabulky je zřejmé, že plné ochrany dosahují jen VPN služby placené a od společností zaměřených přímo na ně. V případě VPN služeb od antivirových společností již bylo dosahováno smíšených výsledků. Kdy nejlépe dopadla VPN služba od české společnosti Avast. V případě VPN služby zdarma (Opera VPN), již bylo nalezených nedostatků více.

Tabulka č. 7 – Porovnání výsledků VPN služeb (zdroj: vlastní)

Název VPN služby	Počet získaných bodů
NordVPN	11
SurfShark	11
ExpressVPN	10,5
Perfect-Privacy	9
IP-Vanish	9,5
Avast Secureline	9
Proton VPN	9
AVG VPN	6,5
Norton Wifi Privacy	6
Kaspersky VPN	7,5
Opera VPN	4

Z výsledného hodnocení je zřejmé, že jen 2 VPN služby (NordVPN a SurfShark) poskytují uživateli maximální anonymitu. Obě tyto služby uspěly ve všech hodnocených kategoriích. Ve všech ostatních případech byly nalezeny nedostatky. V případě ExpressVPN se jednalo jen o nedostatečnou možnost mít připojeno více zařízení současně. V ostatních ohledech dosáhl taktéž bezchybného výsledku.

Jak je dále zřejmé VPN služby zaměřené čistě na poskytování této služby dopadly ve srovnání lépe. VPN služby od primárně antivirových společností již obsahovaly řadu nedostatků a bezpečnostních rizik. V případě bezplatné VPN služby OperaVPN bylo nedostatků nalezeno nejvíce. Zde je možná na zvážení, zdali tato služba oproti klasickému internetovému připojení nabízí nějakou ochranu.

V případě VPN služby se tedy vyplatí vybrat ověřeného poskytovatele se zaměřením na bezpečnost uživatelů i za mnohdy vyšší cenu. Ostatní služby sice nabízí prvek ochrany, nicméně nedostatečný.

7 NÁVRHY PŘÍSTUPŮ UŽIVATELE K PROBLEMATICE DIGITÁLNÍ STOPY A ŠEDÝCH DAT

Digitální stopu za sebou uživatel zanechává při každém pohybu na internetu. Nicméně s využitím správných nástrojů je možné ji částečně skrýt. Úplné zamezení vzniku digitální stopy je nemožné. Snad jen při úplné absenci užívání internetu. I zde to nicméně neplatí stoprocentně, jelikož naše digitální stopa může vznikat i díky ostatním. Například přátelé, kteří na sociální síti sdílí skupinové foto. Nebo i při úniku dat od poskytovatele služby kterou využíváme v off-line světě. Úplnému zamezení vzniku digitální stopy tedy není možné předejít. Nicméně omezení digitální stopy možné je. Vykoupeno je to pro uživatele nižším komfortem při užívání internetu. Tato míra omezení do jisté míry určuje i míru digitálních stop, které je možné následně zjistit. Platí zde, že opravdu účinné nástroje pro omezení digitální stopy, jsou pro každodenní použití ne moc použitelné.

7.1 Promiskuitní přístup – žádná ochrana

V případě, že uživatel není ochoten investovat čas a úsilí do své vlastní ochrany při pohybu online je jeho digitální stopa velmi výrazná. Nejpoužívanější prohlížeče, jak bylo zjištěno v kapitole 5 neposkytují dostatečnou ochranu. Absence dalších prvků, jako jsou nástroje a VPN služba umožňuje snadné sledování, včetně reálné IP adresy uživatele.

Už i volba bezpečnějšího prohlížeče (Firefox, Brave) by zde znamenala výrazný skok v bezpečnosti a anonymitě uživatele.

7.2 Liberální přístup – vybraný prohlížeč a nástroj

V případě využití výsledků z kapitoly 5 a to využití bezpečného prohlížeče (Firefox a Brave) a následné instalaci nástroje blokujícího sledovací prvky dochází již k posunu v oblasti minimalizace digitální stopy. Volba prohlížeče a nástroje zde hraje důležitou roli. V případě nástroje je nutné vybrat si nástroj od ověřeného vydavatele s otevřeným kódem, který uživateli zajistí minimalizaci možnosti nekalých praktik vydavatele, nebo zneužití bezpečnostních děr. Při srovnání nástrojů blokujících sledovací prvky vyšel nejlépe nástroj Ghostery, který na pouhých 10 nejnavštěvovanějších stránkách nalezl a blokoval 48 prvků.

V kombinaci s bezpečným prohlížečem je zde již uživateli poskytována určitá forma ochrany před záznamem jeho digitální stopy. Nicméně stále je zde problém s viditelnou reálnou IP adresou, pro kterou je nutné využití jiného softwaru.

7.3 Liberálně paranoidní přístup – použití vybraného prohlížeče, nástroje a virtuální privátní sítě

V případě využití základních opatření rozepsaných v předchozí kapitole, dochází stále k úniku reálné IP adresy uživatele. Tento problém je možné vyřešit využitím VPN služby. Jak je zřejmé ze srovnání VPN služeb v kapitole 6, málokterá i placená služba ovšem nabízí reálnou anonymitu.

V případě, kdy uživatel chce dosáhnout skrytí své reálné IP adresy bez pravidelné platby, je odkázán na VPN služby, poskytované zdarma. Nicméně jak je vidět na srovnání, kde byla srovnávána i služba Opera VPN, jakožto zástupce VPN služeb poskytovaných zdarma, obsahuje tato služba mnoho nedostatků. Ve srovnání dopadla služba zdarma zdaleka nejhůře, kdy kromě nedostatků v oblasti bezpečnosti zde byl problém i s rychlostí, a tedy i použitelností služby.

V případě využití VPN služby od antivirové společnosti, byly výsledky již o něco lepší, nicméně na to, že se jedná o placenou službu, je možné dosáhnout lepších výsledků při zvolení VPN služby přímo od společnosti zaměřené jen na tuto oblast. Jako nejlepší možnosti se po srovnání jeví služby NordVPN a SurfShark. Ty již nabízejí uživateli značnou míru anonymity online a tedy i minimalizaci jeho digitální stopy.

Při využití bezpečného prohlížeče například prohlížeče Firefox, spolu s nástrojem Ghostery a VPN službou NordVPN je uživateli poskytována již značná míra anonymity. A oproti uživateli využívající jen standartní webový prohlížeč i výrazně menší záznam digitální stopy.

7.4 Paranoidní přístup

Pokud by ovšem uživateli nestačilo ani spojení popsané v předchozí kapitole zbývá mu jen jedna možnost. A to využití sítě TOR. Ta nabízí díky několika vrstvám šifrování ještě vyšší míru anonymity online. To je nicméně vykoupeno nefunkčností některých webů a taktéž výrazně pomalejší rychlostí připojení. Proto osobně nevidím použití tohoto nástroje pro každodenní využití reálné. Nicméně v případě nutnosti maximální míry anonymity a prakticky nulové digitální stopy je možné tohoto nástroje využít, ideálně v kombinaci s operačním systémem Tails, díky kterému nezůstanou stopy ani v samotném zařízení, ze kterého bylo k webu přistupováno. Nicméně využití této kombinace s sebou nese značná omezení pro uživatele a je tak pro každodenní použití nevhodné.

ZÁVĚR

V oblasti šedých dat existuje mnoho nesrovnalostí. Je to dáno primárně tím, že neexistuje přesná a platná definice pro tuto oblast. I v Evropě je pohled na to, co to šedá data jsou, roztříštěn. Zároveň tomuto problému není přikládán v oblasti bezpečnosti dostatečný význam. Nicméně v budoucnu, s dalším rozvojem umělé inteligence a strojového učení, přibudou nové metody, jak tato šedá data třídit, analyzovat a také de-anonymizovat. To je spojené i s neustále rostoucím množstvím těchto dat. S přesunem každodenních aktivit do online prostoru, dochází doslova na každém rohu, k jejich záznamu. Pro minimalizaci těchto dat je nutné, se tedy zaměřit na aktivní přístup. Tedy na snahu o jejich anonymizaci, nebo o to, aby nebyla vůbec zaznamenávána. K tomu uživateli mohou posloužit nástroje vhodné pro skrytí digitální stopy.

V případě digitální stopy bylo zjištěno, že úplně vymazat, ji při používání internetu nelze. I v případě, kdy by uživatelem nebyl internet vůbec využíván, mu vzniká digitální stopa. V tomto případě se může jednat o záznamy na úřadech, ubytování v hotelech, nebo i záznamy na sociálních sítích, kdy například rodinný příslušník přidá společnou fotografii.

S přihlédnutím na schopnosti běžného uživatele bylo přistoupeno ke třem základním prvkům. Porovnání webových prohlížečů, jakožto brány do online světa. Možnosti v oblasti nástrojů pro zabránění sledování ve vybraných prohlížečích. A v posledním případě i skrytí reálné IP adresy dostupnými nástroji.

V případě webových prohlížečů se ukázalo, že ty nejpoužívanější (Chrome, Edge) obsahují značné množství nedostatků. Jako nejlepší, ale zároveň použitelné prohlížeče pro každodenní aktivity, se ukázaly prohlížeče Brave a Firefox. Oba byly vytvořeny s ohledem na bezpečnost a anonymitu uživatele, což dokázaly i svým výsledkem ve srovnání.

Výběrem webového prohlížeče nicméně cesta k minimalizaci digitální stopy nekončí. I při výběru bezpečného prohlížeče, je uživatel stále sledován a jeho digitální stopa snadno čitelná. Pro lepší výsledek je nutné instalovat rozšíření na blokování sledovacích prvků. Ve srovnání jako nejlepší vyšel nástroj Ghostery. Ten, při navštívení deseti nejnavštěvovanějších stránek v České republice nalez a částečně zablokoval 48 prvků.

Posledním bodem, který bylo nutné vyřešit, byl únik reálné IP adresy uživatele. Zde se jako nejlepší řešení jeví, použití placené VPN služby. Při použití obdobné, ale neplacené služby, kdy v této práci byla porovnávána služba OperaVPN, nedochází ani zdaleka k dostatečné ochraně. Ve srovnání vyšly jako nejlepší VPN služby NordVPN a SurfShark. Tyto služby

již nabízí dobrou úroveň anonymity, kdy u nich nebyly nalezeny problémy, ani v jednom z porovnávaných bodů.

Při použití všech třech prvků ochrany: webový prohlížeč Brave nebo Firefox, nástroj Ghostery a VPN služba NordVPN nebo SurfShark, již dochází ke značné minimalizaci vzniku šedých dat a digitální stopy uživatele, stejně tak i k jejímu částečnému anonymizování. Instalace výše zmíněných prvků ochrany, je bezproblémová i pro uživatele bez hlubších znalostí informačních technologií. A i proto by se užívání vybraných nástrojů, nebo nástrojů jim podobných, mělo stát standardem při práci a zábavě v online světě. Na základě zpracování bakalářské práce byly cíle, vytyčené v úvodu práce, zcela naplněny.

SEZNAM POUŽITÉ LITERATURY

ABRAHAM, Stephanie et al., 2016. *Tails & Tor ... and other tools for Safeguarding Online Activities* [online]. [cit. 2022-03-16]. Dostupné z: https://arxiv.org/ftp/arxiv/papers/1710/1710.08705.pdf

ABUKAR, Yahye a Mohd AIZAINI, 2014. *Survey of Keylogger technologies* [online]. [cit. 2022-02-02]. Dostupné z: https://www.researchgate.net/profile/Yahye-Abukar/publication/309230926_Survey_of_Keylogger_Technologies/links/59a00619aca27237edba3c12/Survey-of-Keylogger-Technologies.pdf. Universiti Teknologi Malaysia.

BLACK, Paul, 2022. *Top 13 most secure browsers for your privacy in 2022* [online]. [cit. 2022-03-12]. Dostupné z: https://nordvpn.com/blog/best-privacy-browser/

BORGMAN, Christine, 2018. *Open Data, Grey Data, and Stewardship: Universities at the Privacy Frontier* [online]. Berkeley Technology Law Journal, 365 s. [cit. 2022-02-04]. DOI: 10.15779/Z38B56D489. Dostupné z: https://lawcat.berkeley.edu/record/1128546. University of California, Los Angeles.

BROOKS, Charles J. et al., [2018]. *Cybersecurity essentials*. Indianapolis, Indiana: Sybex, John Wiley. ISBN 978-1-119-36239-5.

Browser Privacy Test [online], 2021. [cit. 2022-04-10]. Dostupné z: https://webbrowsertools.com/privacy-test/

DEAN, Brian, 2021. *Web Browser Market Share In 2022: 85+ Browser Usage Statistics* [online]. [cit. 2022-03-12]. Dostupné z: https://backlinko.com/browser-market-share

FISH, Tony, 2013. *Digital footprints* [online]. [cit. 2021-12-01]. Dostupné z: https://www.phil.muni.cz/journals/index.php/proinflow/article/view/2013-1-9/922

FORTE, Dario, 2006. *Advances in Onion Routing: Description and backtracing/ investigation problems* [online]. [cit. 2022-03-16]. Dostupné z: https://reader.elsevier.com/reader/sd/pii/S1742287606000272?token=2EE67F8752B5E80A11A2B9113993A7C60F1CB7B69673D7B8E94B4984D9C297D395708800C211A2C42BF4D3D3C8A73B31&originRegion=eu-west-1&originCreation=20220316133826

GREEN, Emily, 2021. *12 types of social engineering attacks* [online]. [cit. 2022-03-11]. Dostupné z: https://nordvpn.com/blog/social-engineering/

HILLSON, Shannon, 2021. *The Most Important Differences Between First-Party vs Third-Party Cookies* [online]. [cit. 2022-02-02]. Dostupné z: https://quicklearnacademy.com/blog/first-party-vs-third-party-cookies/

History of keyloggers [online]. [cit. 2022-02-02]. Dostupné z: https://www.malwarebytes.com/keylogger

HO, Rachel, 2022. *10 Most Secure Web Browsers in 2022: Ranked + Rated* [online]. [cit. 2022-03-13]. Dostupné z: https://www.safetydetectives.com/blog/which-is-the-most-secure-web-browser-to-use-in/

HTTPS [online]. [cit. 2022-04-10]. Dostupné z: https://cs.wikipedia.org/wiki/HTTPS

CHIVERS, Kyle, 2021. *What does an IP address tell you and how it can put you at risk* [online]. [cit. 2022-03-11]. Dostupné z: https://us.norton.com/internetsecurity-privacy-what-does-an-ip-address-tell-you.html

IP Address Lookup – IP Lookup Tool [online], 2022. [cit. 2022-05-05]. Dostupné z: https://www.whatismyip.com/ip-address-lookup/

JADOON, Abid Khan et al., 2019. *Forensic Analysis of Tor Browser: A Case Study for Privacy and Anonymity on the Web* [online]. [cit. 2022-03-15]. 0379-0738. Dostupné z: https://www.sciencedirect.com/science/article/pii/S0379073819301082?casa_token=RU5GTe0stBYAAAAA:jIo8H5M4AB_33JfzalSDgWRp--WQlvQEoR9_l1Wv-VX00e6POL9JY446IjsygZpyWHS7IjGLLPA

JOHNSON, Allie, 2022. *What is a no-log VPN?* [online]. [cit. 2022-04-24]. Dostupné z: https://us.norton.com/internetsecurity-privacy-what-is-a-no-log-vpn.html
KOLOUCH, Jan a Pavel BAŠTA, 2019. *CyberSecurity* [online]. Praha: CZ.NIC, z.s.p.o. [cit. 2022-03-12]. CZ.NIC. ISBN 978-80-88168-34-8. Dostupné z: https://knihy.nic.cz/files/edice/cybersecurity.pdf
KOVÁŘOVÁ, Pavla, 2019. *Informační bezpečnost žáků základních škol* [online]. [cit. 2022-02-02]. Dostupné z: https://digilib.phil.muni.cz/bitstream/handle/11222.digilib/141117/SpisyFF_489-2019-1_5.pdf?sequence=1
KRÁL, Mojmír, 2006. *Bezpečnost domácího počítače: prakticky a názorně*. Praha: Grada. Průvodce (Grada). ISBN 80-247-1408-6.
KUMAR, Arun, 2020. *How can a Browser Sandbox protect your computer?* [online]. [cit. 2022-04-10]. Dostupné z: https://www.thewindowsclub.com/what-is-browser-sandbox
Malware [online], 2022. [cit. 2022-04-22]. Dostupné z: https://www.malwarebytes.com/malware
MARDISAL, Rob, 2021. *The Best VPN Services (2021)* [online]. [cit. 2022-04-25]. Dostupné z: https://thebestvpn.com/
MITNICK, Kevin a Robert VAMOSI, 2019. *The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data*. ISBN 978-0-316-38052-2.
Národní úřad pro kybernetickou a informační bezpečnost, 2021. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020* [online]. [cit. 2022-05-05].
PAVLENKO, Daria, Leonid BARYKIN a Kazbek DADTEE, 2021. *Collection and analysis of digital footprints in LMS* [Procedia Computer Science]. Volume 190. Elsevier [cit. 2022-02-01]. ISSN 1877-0509. Dostupné z: https://www.sciencedirect.com/science/article/pii/S1877050921013612
PIAZZA, Dan, 2020. *What is DNS over HTTPS (DoH) & How to Enable in Windows 10* [online]. [cit. 2022-04-10]. Dostupné z: https://stealthbits.com/blog/dns-over-https/
RAMIREZ, Misael, 2020. *What is a Virtual Private Network and How Does it Work?* [online]. [cit. 2022-03-19]. Dostupné z: https://www.liquidweb.com/kb/what-is-a-virtual-private-network-and-how-does-it-work/
SAVIĆ, Dobrica, 2019. *When is 'grey' too 'grey'? A case of grey data* [online]. [cit. 2022-02-03]. Dostupné z: https://www.researchgate.net/publication/340096377_When_is_'grey'_too_'grey'_A_case_of_grey_data
Server Log Files in a Nutshell [online], 2020. [cit. 2022-02-01]. Dostupné z: https://www.graylog.org/post/server-log-files-in-a-nutshell
SKOČEK, Jakub, 2012. *Digitální stopy, možnost kontroly a eliminace pomocí volně dostupných vybraných nástrojů* [online]. Praha [cit. 2022-02-01]. Dostupné z: https://dspace.cuni.cz/bitstream/handle/20.500.11956/40626/130082021.pdf?sequence=1&isAllowed=y. Bakalářská práce. Univerzita Karlova v Praze.
SKOČEK, Jakub, 2015. *Digitální identita v době služeb Google* [online]. Praha [cit. 2022-02-06]. Dostupné z: https://dspace.cuni.cz/bitstream/handle/20.500.11956/81169/120195681.pdf?sequence=1&isAllowed=y. Diplomová práce. Univerzita Karlova v Praze.
SVEN, Taylor, 2021. *How to Fix WebRTC Leaks (All Browsers)* [online]. [cit. 2022-03-13]. Dostupné z: https://restoreprivacy.com/webrtc-leaks/
SVEN, Taylor, 2021. *Top 10 Secure Browsers That Protect Your Privacy in 2022* [online]. [cit. 2022-03-18]. Dostupné z: https://restoreprivacy.com/browser/secure/

ŠULC, Vladimír, 2018. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 978-80-7380-737-5.
TOLSON, Bill, 2016. *The Lifecycle of Grey Data* [online]. [cit. 2022-02-03]. Dostupné z: https://www.archive360.com/blog/the-lifecycle-of-grey-data
VARVELLO, Matteo et al., 2021. *VPN-Zero: A Privacy-Preserving Decentralized Virtual Private Network* [online]. [cit. 2022-03-18]. Dostupné z: https://ieeexplore.ieee.org/abstract/document/9472843?casa_token=AfgDwoSOhDwAAAAA:337AuHAUbb9iQHlwJOw5Js15sdLdRoUjky4eZmL8eTvH7JwPzaj1LXIA6WWRAnU6h8ysiNPASGE
Visual Traceroute [online], 2021. [cit. 2022-05-05]. Dostupné z: https://gsuite.tools/traceroute
WebBrowserTools [online], 2021. [cit. 2022-05-05]. Dostupné z: https://webbrowsertools.com/
What are cookies [online], 2022. [cit. 2022-02-01]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/cookies
What is open source? [online]. [cit. 2022-04-10]. Dostupné z: https://opensource.com/resources/what-open-source
WHITMORE, Charles, 2022. *How to disable WebRTC and prevent leaks* [online]. [cit. 2022-04-10]. Dostupné z: https://nordvpn.com/blog/webrtc/
Zákon č. 127/2005 Sb. [online], 2005. Česká republika [cit. 2022-03-13]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-127
ZHIPENG, Zhang et al., 2018. *VPN: a Boon or Trap? : A Comparative Study of MPLS, IPSec, and SSL Virtual Private Networks* [online]. [cit. 2022-03-18]. Dostupné z: https://ieeexplore.ieee.org/abstract/document/8487653?casa_token=uJrOP0jTFnEAAAAA:8ENVswsBrNp--sdUAXjxs-qLjbx5zMPtoplpKNtMOgaRkV1G5BdX1c6_85diD5RAPEZZTp45-3o
ŽAŽO, Daniel, 2015. *Digitální stopy, identita a její ochrana* [online]. Ostrava [cit. 2022-02-01]. Dostupné z: https://dspace.vsb.cz/bitstream/handle/10084/108631/ZAZ004_FEI_N2647_2612T025_2015.pdf?sequence=1&isAllowed=y. Diplomová práce. VŠB – Technická univerzita Ostrava.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AES-CBC – Advanced Encryption Standard Cipher block chaining

CGOC – Compliance, Governance and Oversight

DDoS – Denial of Service

DNS – Systém doménových jmen

DOH – DNS přes HTTPS

dVPN – decentralizovaná virtuální privátní síť

EU – Evropská Unie

GB – Gigabyte

Gbs – Gigabitů za sekundu

GDPR – General Data Protection regulation

GPS – Globální družicový polohový systém

HTTP – Hypertext Transfer Protocol

HTTPS – Hypertext Transfer Protocol Secure

CHAP – Challenge Handshake Authentication Protocol

IBM – International Business Machines Corporation

IETF – Internet Engineering Task Force

IP – Internet protokol

IPSec – Internet Protocol Security Virtual Private Network

IPv4 – Internet protokol verze 4

IPv6 – Internet protokol verze 6

macOS – Operační systém pro počítače Macintosh společnosti Apple

MB – Megabyte

MPLS VPN – Multiprotocol Label Switching Virtual Private Network

MS-CHAP-v2 – Microsoft Challenge Handshake Authentication Protocol version 2

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost

OSI – Open Systém Interconection

P2P – Peer-to-Peer

RSA – Rivest–Shamir–Adleman

SSL – Secure Sockets Layer

SWGDE – Scientific Working Group on Digital Evidence

Tails – The Amnesic Incognito Live Systém

TLS – Transport Layer Security

TOR – The Onion Router

URL – Uniform Resource Locator

UTB – Univerzita Tomáše Bati

VPN – Virtuální privátní síť

WebRTC – Web Real-Time Communication

SEZNAM OBRÁZKŮ

SEZNAM TABULEK